

# Interpolation synthesis for quadratic polynomial inequalities and combination with *EUF*

Ting Gan<sup>1</sup>, Liyun Dai<sup>1</sup>, Bican Xia<sup>1</sup>, Naijun Zhan<sup>2</sup>, Deepak Kapur<sup>3</sup>, and Mingshuai Chen<sup>2</sup>

<sup>1</sup> LMAM & School of Mathematical Sciences, Peking University  
`{gant, dailiyun, xbc}@pku.edu.cn`,

<sup>2</sup> State Key Lab. of Computer Science, Institute of Software, CAS  
`znj@ios.ac.cn`

<sup>3</sup> Department of Computer Science, University of New Mexico  
`kapur@cs.unm.edu`

**Abstract.** An algorithm for generating interpolants for formulas which are conjunctions of quadratic polynomial inequalities (both strict and nonstrict) is proposed. The algorithm is based on a key observation that quadratic polynomial inequalities can be linearized if they are concave. A generalization of Motzkin’s transposition theorem is proved, which is used to generate an interpolant between two mutually contradictory conjunctions of polynomial inequalities, using semi-definite programming in time complexity  $\mathcal{O}(n^3 + nm)$  with a given threshold, where  $n$  is the number of variables and  $m$  is the number of inequalities. Using the framework proposed by [21] for combining interpolants for a combination of quantifier-free theories which have their own interpolation algorithms, a combination algorithm is given for the combined theory of concave quadratic polynomial inequalities and the equality theory over uninterpreted functions symbols (*EUF*). The proposed approach is applicable to all existing abstract domains like *octagon*, *polyhedra*, *ellipsoid* and so on, therefore it can be used to improve the scalability of existing verification techniques for programs and hybrid systems. In addition, we also discuss how to extend our approach to formulas beyond concave quadratic polynomials using Gröbner basis.

**Keywords:** Program verification, Interpolant, Concave quadratic polynomials, Motzkin’s theorem, Semi-definite programming.

## 1 Introduction

Interpolants have been popularized by McMillan [15] for automatically generating invariants of programs. Since then, developing efficient algorithms for generating interpolants for various theories has become an active area of research; in particular, methods have been developed for generating interpolants for Presburger arithmetic (both for integers as well as for rationals/reals), theory of equality over uninterpreted symbols as well as their combination. Most of these methods assume the availability of a refutation proof of  $\alpha \wedge \beta$  to generate a “reverse” interpolant of  $(\alpha, \beta)$ ; calculi have been proposed to label an inference node in a refutational proof depending upon whether symbols of formulas on which the inference is applied are purely from  $\alpha$  or  $\beta$ . For propositional calculus, there already existed methods for generating interpolants from resolution proofs [11,16] prior to McMillan’s work, which generate different interpolants

from those done by McMillan’s method. This led D’Silva et al [6] to study strengths of various interpolants.

In Kapur, Majumdar and Zarba [10], an intimate connection between interpolants and quantifier elimination was established. Using this connection, existence of quantifier-free as well as interpolants with quantifiers were shown for a variety of theories over container data structures. A CEGAR based approach was generalized for verification of programs over container data structures using interpolants. Using this connection between interpolant generation and quantifier elimination, Kapur [9] has shown that interpolants form a lattice ordered using implication, with the interpolant generated from  $\alpha$  being the bottom of such a lattice and the interpolant generated from  $\beta$  being the top of the lattice.

Nonlinear polynomial inequalities have been found useful to express invariants for software involving sophisticated number theoretic functions as well as hybrid systems; an interested reader may see [27,28] where different controllers involving nonlinear polynomial inequalities are discussed for some industrial applications.

We propose an algorithm to generate interpolants for quadratic polynomial inequalities (including strict inequalities). Based on the insight that for analyzing the solution space of concave quadratic polynomial (strict) inequalities, it suffices to linearize them. We prove a generalization of Motzkin’s transposition theorem to be applicable for quadratic polynomial inequalities (including strict as well as nonstrict). Based on this result, we prove the existence of interpolants for two mutually contradictory conjunctions  $\alpha, \beta$  of concave quadratic polynomial inequalities and give an algorithm for computing an interpolant using semi-definite programming. The algorithm is recursive with the basis step of the algorithm relying on an additional condition on concave quadratic polynomials appearing in nonstrict inequalities that any nonpositive constant combination of these polynomials is never a nonzero sum of square polynomial (called **NSOSC**). In this case, an interpolant output by the algorithm is either a strict inequality or a nonstrict inequality much like in the linear case. In case, this condition is not satisfied by the nonstrict inequalities, i.e., there is a nonpositive constant combinations of polynomials appearing as nonstrict inequalities that is a negative of a sum of squares, then new mutually contradictory conjunctions of concave quadratic polynomials in fewer variables are derived from the input augmented with the equality relation deduced, and the algorithm is recursively invoked on the smaller problem. The output of this algorithm is in general an interpolant that is a disjunction of conjunction of polynomial nonstrict or strict inequalities. The **NSOSC** condition can be checked in polynomial time using semi-definite programming.

We also show how separating terms  $t^-, t^+$  can be constructed using common symbols in  $\alpha, \beta$  such that  $\alpha \Rightarrow t^- \leq x \leq t^+$  and  $\beta \Rightarrow t^+ \leq y \leq t^-$ , whenever  $(\alpha \wedge \beta) \Rightarrow x = y$ . Similar to the construction for interpolants, this construction has the same recursive structure with concave quadratic polynomials satisfying **NSOSC** as the basis step. This result enables the use of the framework proposed in [17] based on hierarchical theories and a combination method for generating interpolants by Yorsh and Musuvathi, from combining equality interpolating quantifier-free theories for generating interpolants for the combined theory of quadratic polynomial inequalities and theory of uninterpreted symbols.

Obviously, our results are significant in program verification as all well-known abstract domains, e.g. *octagon*, *polyhedra*, *ellipsoid* and so on, which are widely used in the verification of programs and hybrid systems, are *quadratic* and *concave*. In addition, we also discuss the possibility to extend our results to general polynomial formulas by allowing polynomial equalities whose polynomials may be neither *concave* nor *quadratic* using Gröbner basis.

We develop a combination algorithm for generating interpolants for the combination of concave quadratic polynomial inequalities and uninterpreted function symbols.

In [5], Dai et al. gave an algorithm for generating interpolants for conjunctions of mutually contradictory nonlinear polynomial inequalities based on the existence of a witness guaranteed by Stengle’s **Positivstellensatz** [22] that can be computed using semi-definite programming. Their algorithm is incomplete in general but if every variables ranges over a bounded interval (called Archimedean condition), then their algorithm is complete. A major limitation of their work is that formulas  $\alpha, \beta$  cannot have uncommon variables<sup>4</sup>. However, they do not give any combination algorithm for generating interpolants in the presence of uninterpreted function symbols appearing in  $\alpha, \beta$ .

The paper is organized as follows. After discussing some preliminaries in the next section, Section 3 defines concave quadratic polynomials, their matrix representation and their linearization. Section 4 presents the main contribution of the paper. A generalization of Motzkin’s transposition theorem for quadratic polynomial inequalities is presented. Using this result, we prove the existence of interpolants for two mutually contradictory conjunctions  $\alpha, \beta$  of concave quadratic polynomial inequalities and give an algorithm (Algorithm 2) for computing an interpolant using semi-definite programming. Section 5 extends this algorithm to the combined theory of concave quadratic inequalities and *EUF* using the framework used in [21,17]. Implementation and experimental results using the proposed algorithms are briefly reviewed in Section 6, and we conclude and discuss future work in Section 7.

## 2 Preliminaries

Let  $\mathbb{N}$ ,  $\mathbb{Q}$  and  $\mathbb{R}$  be the set of natural, rational and real numbers, respectively. Let  $\mathbb{R}[\mathbf{x}]$  be the polynomial ring over  $\mathbb{R}$  with variables  $\mathbf{x} = (x_1, \dots, x_n)$ . An atomic polynomial formula  $\varphi$  is of the form  $p(\mathbf{x}) \diamond 0$ , where  $p(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ , and  $\diamond$  can be any of  $=, >, \geq, \neq$ ; without any loss of generality, we can assume  $\diamond$  to be any of  $>, \geq$ . An arbitrary polynomial formula is constructed from atomic ones with Boolean connectives and quantifications over real numbers. Let  $\mathbf{PT}(\mathbb{R})$  be a first-order theory of polynomials with real coefficient, In this paper, we are focusing on quantifier-free fragment of  $\mathbf{PT}(\mathbb{R})$ .

Later we discuss quantifier-free theory of equality of terms over uninterpreted function symbols and its combination with the quantifier-free fragment of  $\mathbf{PT}(\mathbb{R})$ . Let  $\Sigma$  be a set of (new) function symbols. Let  $\mathbf{PT}(\mathbb{R})^\Sigma$  be the extension of the quantifier-free theory with uninterpreted function symbols in  $\Sigma$ .

For convenience, we use  $\perp$  to stand for *false* and  $\top$  for *true* in what follows.

<sup>4</sup> See however an expanded version of their paper under preparation where they propose heuristics using program analysis for eliminating uncommon variables.

**Definition 1.** A model  $\mathcal{M} = (M, f_{\mathcal{M}})$  of  $\mathbf{PT}(\mathbb{R})^{\Sigma}$  consists of a model  $M$  of  $\mathbf{PT}(\mathbb{R})$  and a function  $f_{\mathcal{M}} : \mathbb{R}^n \rightarrow \mathbb{R}$  for each  $f \in \Sigma$  with arity  $n$ .

**Definition 2.** Let  $\phi$  and  $\psi$  be formulas of a considered theory  $\mathcal{T}$ , then

- $\phi$  is valid w.r.t.  $\mathcal{T}$ , written as  $\models_{\mathcal{T}} \phi$ , iff  $\phi$  is true in all models of  $\mathcal{T}$ ;
- $\phi$  entails  $\psi$  w.r.t.  $\mathcal{T}$ , written as  $\phi \models_{\mathcal{T}} \psi$ , iff for any model of  $\mathcal{T}$ , if  $\psi$  is true in the model, so is  $\phi$ ;
- $\phi$  is satisfiable w.r.t.  $\mathcal{T}$ , iff there exists a model of  $\mathcal{T}$  such that in which  $\phi$  is true; otherwise unsatisfiable.

Note that  $\phi$  is unsatisfiable iff  $\phi \models_{\mathcal{T}} \perp$ .

Craig showed that given two formulas  $\phi$  and  $\psi$  in a first-order theory  $\mathcal{T}$  such that  $\phi \models \psi$ , there always exists an *interpolant*  $I$  over the common symbols of  $\phi$  and  $\psi$  such that  $\phi \models I$ ,  $I \models \psi$ . In the verification literature, this terminology has been abused following [15], where an *reverse interpolant*  $I$  over the common symbols of  $\phi$  and  $\psi$  is defined for  $\phi \wedge \psi \models \perp$  as:  $\phi \models I$  and  $I \wedge \psi \models \perp$ .

**Definition 3.** Let  $\phi$  and  $\psi$  be two formulas in a theory  $\mathcal{T}$  such that  $\phi \wedge \psi \models_{\mathcal{T}} \perp$ . A formula  $I$  said to be a (reverse) interpolant of  $\phi$  and  $\psi$  if the following conditions hold:

- i  $\phi \models_{\mathcal{T}} I$ ;
- ii  $I \wedge \psi \models_{\mathcal{T}} \perp$ ; and
- iii  $I$  only contains common symbols and free variables shared by  $\phi$  and  $\psi$ .

If  $\psi$  is closed, then  $\phi \models_{\mathcal{T}} \psi$  iff  $\phi \wedge \neg\psi \models_{\mathcal{T}} \perp$ . Thus,  $I$  is an interpolant of  $\phi$  and  $\psi$  iff  $I$  is a reverse interpolant of  $\phi$  and  $\neg\psi$ . In this paper, we just deal with reverse interpolant, and from now on, we abuse interpolant and reverse interpolant.

## 2.1 Motzkin's transposition theorem

Motzkin's transposition theorem [18] is one of the fundamental results about linear inequalities; it also served as a basis of the interpolant generation algorithm for the quantifier-free theory of linear inequalities in [17]. The theorem has several variants as well. Below we give two of them.

**Theorem 1 (Motzkin's transposition theorem [18]).** Let  $A$  and  $B$  be matrices and let  $\alpha$  and  $\beta$  be column vectors. Then there exists a vector  $\mathbf{x}$  with  $A\mathbf{x} \geq \alpha$  and  $B\mathbf{x} > \beta$ , iff

- for all row vectors  $\mathbf{y}, \mathbf{z} \geq 0$  :
- (i) if  $\mathbf{y}A + \mathbf{z}B = 0$  then  $\mathbf{y}\alpha + \mathbf{z}\beta \leq 0$ ;
  - (ii) if  $\mathbf{y}A + \mathbf{z}B = 0$  and  $\mathbf{z} \neq 0$  then  $\mathbf{y}\alpha + \mathbf{z}\beta < 0$ .

**Corollary 1.** Let  $A \in \mathbb{R}^{r \times n}$  and  $B \in \mathbb{R}^{s \times n}$  be matrices and  $\alpha \in \mathbb{R}^r$  and  $\beta \in \mathbb{R}^s$  be column vectors. Denote by  $A_i, i = 1, \dots, r$  the  $i$ th row of  $A$  and by  $B_j, j = 1, \dots, s$

the  $j$ th row of  $B$ . Then there does not exist a vector  $\mathbf{x}$  with  $A\mathbf{x} \geq \boldsymbol{\alpha}$  and  $B\mathbf{x} > \boldsymbol{\beta}$ , iff there exist real numbers  $\lambda_1, \dots, \lambda_r \geq 0$  and  $\eta_0, \eta_1, \dots, \eta_s \geq 0$  such that

$$\sum_{i=1}^r \lambda_i (A_i \mathbf{x} - \alpha_i) + \sum_{j=1}^s \eta_j (B_j \mathbf{x} - \beta_j) + \eta_0 \equiv 0, \quad (1)$$

$$\sum_{j=0}^s \eta_j > 0. \quad (2)$$

*Proof.* The “if” part is obvious. Below we prove the “only if” part.

By Theorem 1, if  $A\mathbf{x} \geq \boldsymbol{\alpha}$  and  $B\mathbf{x} > \boldsymbol{\beta}$  have no common solution, then there exist two row vectors  $\mathbf{y} \in \mathbb{R}^r$  and  $\mathbf{z} \in \mathbb{R}^s$  with  $\mathbf{y} \geq 0$  and  $\mathbf{z} \geq 0$  such that

$$(\mathbf{y}A + \mathbf{z}B = 0 \wedge \mathbf{y}\boldsymbol{\alpha} + \mathbf{z}\boldsymbol{\beta} > 0) \vee (\mathbf{y}A + \mathbf{z}B = 0 \wedge \mathbf{z} \neq 0 \wedge \mathbf{y}\boldsymbol{\alpha} + \mathbf{z}\boldsymbol{\beta} \geq 0).$$

Let  $\lambda_i = y_i, i = 1, \dots, r, \eta_j = z_j, j = 1, \dots, s$  and  $\eta_0 = \mathbf{y}\boldsymbol{\alpha} + \mathbf{z}\boldsymbol{\beta}$ . Then it is easy to check that Eqs. (1) and (2) hold.  $\square$

### 3 Concave quadratic polynomials and their linearization

**Definition 4 (Concave Quadratic).** A polynomial  $f \in \mathbb{R}[\mathbf{x}]$  is called concave quadratic (CQ), if the following two conditions hold:

- (i)  $f$  has total degree at most 2, i.e., it has the form  $f = \mathbf{x}^T A \mathbf{x} + 2\boldsymbol{\alpha}^T \mathbf{x} + a$ , where  $A$  is a real symmetric matrix,  $\boldsymbol{\alpha}$  is a column vector and  $a \in \mathbb{R}$  is a constant;
- (ii) the matrix  $A$  is negative semi-definite, written as  $A \preceq 0$ .<sup>5</sup>

*Example 1.* Let  $g_1 = -x_1^2 + 2x_1 - x_2^2 + 2x_2 - y^2$ , then it can be expressed as

$$g_1 = \begin{pmatrix} x_1 \\ x_2 \\ y \end{pmatrix}^T \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ y \end{pmatrix} + 2 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}^T \begin{pmatrix} x_1 \\ x_2 \\ y \end{pmatrix}.$$

The degree of  $g_1$  is 2, and the corresponding  $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \preceq 0$ . Thus,  $g_1$  is CQ.

It is easy to see that if  $f \in \mathbb{R}[\mathbf{x}]$  is linear, then  $f$  is CQ because its total degree is 1 and the corresponding  $A$  is 0 which is of course negative semi-definite.

A quadratic polynomial can also be represented as an inner product of matrices (cf. [13]), i.e.,  $f(\mathbf{x}) = \left\langle P, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle$ .

<sup>5</sup>  $A$  being negative semi-definite has many equivalent characterizations: for every vector  $\mathbf{x}$ ,  $\mathbf{x}^T A \mathbf{x} \leq 0$ ; every  $k$ th minor of  $A \leq 0$  if  $k$  is odd and  $\geq 0$  otherwise; a Hermitian matrix whose eigenvalues are nonpositive.

### 3.1 Linearization

Consider quadratic polynomials  $f_i$  and  $g_j$  ( $i = 1, \dots, r, j = 1, \dots, s$ ),

$$\begin{aligned} f_i &= \mathbf{x}^T A_i \mathbf{x} + 2\boldsymbol{\alpha}_i^T \mathbf{x} + a_i, \\ g_j &= \mathbf{x}^T B_j \mathbf{x} + 2\boldsymbol{\beta}_j^T \mathbf{x} + b_j, \end{aligned}$$

where  $A_i, B_j$  are symmetric  $n \times n$  matrices,  $\boldsymbol{\alpha}_i, \boldsymbol{\beta}_j \in \mathbb{R}^n$ , and  $a_i, b_j \in \mathbb{R}$ ; let  $P_i := \begin{pmatrix} a_i & \boldsymbol{\alpha}_i^T \\ \boldsymbol{\alpha}_i & A_i \end{pmatrix}$ ,  $Q_j := \begin{pmatrix} b_j & \boldsymbol{\beta}_j^T \\ \boldsymbol{\beta}_j & B_j \end{pmatrix}$  be  $(n+1) \times (n+1)$  matrices, then

$$f_i(\mathbf{x}) = \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle, \quad g_j(x) = \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle.$$

For CQ polynomials  $f_i$ s and  $g_j$ s in which each  $A_i \preceq 0, B_j \preceq 0$ , define

$$K = \{\mathbf{x} \in \mathbb{R}^n \mid f_1(\mathbf{x}) \geq 0, \dots, f_r(\mathbf{x}) \geq 0, g_1(\mathbf{x}) > 0, \dots, g_s(\mathbf{x}) > 0\}. \quad (3)$$

Given a quadratic polynomial  $f(\mathbf{x}) = \left\langle P, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle$ , its *linearization* is defined as  $f(\mathbf{x}) = \left\langle P, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle$ , where  $\begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \succeq 0$ .

Let

$$\overline{\mathbf{X}} = (\mathbf{X}_{(1,1)}, \mathbf{X}_{(2,1)}, \mathbf{X}_{(2,2)}, \dots, \mathbf{X}_{(k,1)}, \dots, \mathbf{X}_{(k,k)}, \dots, \mathbf{X}_{(n,1)}, \dots, \mathbf{X}_{(n,n)})$$

be the vector variable with  $\frac{n(n+1)}{2}$  dimensions corresponding to the matrix  $\mathbf{X}$ . Since  $\mathbf{X}$  is a symmetric matrix,  $\left\langle P, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle$  is a linear expression in  $\mathbf{x}, \overline{\mathbf{X}}$ .

Now, let

$$\begin{aligned} K_1 &= \{\mathbf{x} \mid \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \succeq 0, \wedge_{i=1}^r \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \geq 0, \\ &\quad \wedge_{j=1}^s \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle > 0, \text{ for some } \mathbf{X}\}, \end{aligned} \quad (4)$$

which is the set of all  $\mathbf{x} \in \mathbb{R}^n$  on linearizations of the above  $f_i$ s and  $g_j$ s.

In [7,13], when  $K$  and  $K_1$  are defined only with  $f_i$  without  $g_j$ , i.e., only with non-strict inequalities, it is proved that  $K = K_1$ . By the following Theorem 2, we show that  $K = K_1$  also holds even in the presence of strict inequalities when  $f_i$  and  $g_j$  are CQ. So, when  $f_i$  and  $g_j$  are CQ, the CQ polynomial inequalities can be transformed equivalently to a set of linear inequality constraints and a positive semi-definite constraint.

**Theorem 2.** *Let  $f_1, \dots, f_r$  and  $g_1, \dots, g_s$  be CQ polynomials,  $K$  and  $K_1$  as above, then  $K = K_1$ .*

*Proof.* For any  $\mathbf{x} \in K$ , let  $\mathbf{X} = \mathbf{x}\mathbf{x}^T$ . Then it is easy to see that  $\mathbf{x}, \mathbf{X}$  satisfy (4). So  $\mathbf{x} \in K_1$ , that is  $K \subseteq K_1$ .

Next, we prove  $K_1 \subseteq K$ . Let  $\mathbf{x} \in K_1$ , then there exists a symmetric  $n \times n$  matrix  $\mathbf{X}$  satisfying (4). Because  $\begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \succeq 0$ , we have  $\mathbf{X} - \mathbf{x}\mathbf{x}^T \succeq 0$ . Then by the last two conditions in (4), we have

$$\begin{aligned} f_i(x) &= \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle = \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \left\langle P_i, \begin{pmatrix} 0 & 0 \\ 0 & \mathbf{x}\mathbf{x}^T - \mathbf{X} \end{pmatrix} \right\rangle \\ &= \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \langle A_i, \mathbf{x}\mathbf{x}^T - \mathbf{X} \rangle \geq \langle A_i, \mathbf{x}\mathbf{x}^T - \mathbf{X} \rangle, \\ g_j(x) &= \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle = \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \left\langle Q_j, \begin{pmatrix} 0 & 0 \\ 0 & \mathbf{x}\mathbf{x}^T - \mathbf{X} \end{pmatrix} \right\rangle \\ &= \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \langle B_j, \mathbf{x}\mathbf{x}^T - \mathbf{X} \rangle > \langle B_j, \mathbf{x}\mathbf{x}^T - \mathbf{X} \rangle. \end{aligned}$$

Since  $f_i$  and  $g_j$  are all CQ,  $A_i \preceq 0$  and  $B_j \preceq 0$ . Moreover,  $\mathbf{X} - \mathbf{x}\mathbf{x}^T \succeq 0$ , i.e.,  $\mathbf{x}\mathbf{x}^T - \mathbf{X} \preceq 0$ . Thus,  $\langle A_i, \mathbf{x}\mathbf{x}^T - \mathbf{X} \rangle \geq 0$  and  $\langle B_j, \mathbf{x}\mathbf{x}^T - \mathbf{X} \rangle \geq 0$ . Hence, we have  $f_i(\mathbf{x}) \geq 0$  and  $g_j(\mathbf{x}) > 0$ , so  $\mathbf{x} \in K$ , that is  $K_1 \subseteq K$ .  $\square$

### 3.2 Motzkin's theorem in Matrix Form

If  $\left\langle P, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle$  is seen as a linear expression in  $\mathbf{x}, \overline{\mathbf{X}}$ , then Corollary 1 can be reformulated as:

**Corollary 2.** Let  $\mathbf{x}$  be a column vector variable of dimension  $n$  and  $\mathbf{X}$  be a  $n \times n$  symmetric matrix variable. Suppose  $P_0, P_1, \dots, P_r$  and  $Q_1, \dots, Q_s$  are  $(n+1) \times (n+1)$  symmetric matrices. Let

$$W \triangleq \{(\mathbf{x}, \mathbf{X}) \mid \wedge_{i=1}^r \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \geq 0, \wedge_{j=1}^s \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle > 0\},$$

then  $W = \emptyset$  iff there exist  $\lambda_0, \lambda_1, \dots, \lambda_r \geq 0$  and  $\eta_0, \eta_1, \dots, \eta_s \geq 0$  such that

$$\begin{aligned} \sum_{i=0}^r \lambda_i \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \sum_{j=1}^s \eta_j \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \eta_0 &\equiv 0, \text{ and} \\ \eta_0 + \eta_1 + \dots + \eta_s &> 0. \end{aligned}$$

## 4 Algorithm for generating interpolants for Concave Quadratic Polynomial inequalities

**Problem 1.** Given two formulas  $\phi$  and  $\psi$  on  $n$  variables with  $\phi \wedge \psi \models \perp$ , where

$$\begin{aligned} \phi &= f_1 \geq 0 \wedge \dots \wedge f_{r_1} \geq 0 \wedge g_1 > 0 \wedge \dots \wedge g_{s_1} > 0, \\ \psi &= f_{r_1+1} \geq 0 \wedge \dots \wedge f_r \geq 0 \wedge g_{s_1+1} > 0 \wedge \dots \wedge g_s > 0, \end{aligned}$$

in which  $f_1, \dots, f_r, g_1, \dots, g_s$  are all CQ, develop an algorithm to generate a (reverse) Craig interpolant  $I$  for  $\phi$  and  $\psi$ , on the common variables of  $\phi$  and  $\psi$ , such that  $\phi \models I$

and  $I \wedge \psi \models \perp$ . For convenience, we partition the variables appearing in the polynomials above into three disjoint subsets  $\mathbf{x} = (x_1, \dots, x_d)$  to stand for the common variables appearing in both  $\phi$  and  $\psi$ ,  $\mathbf{y} = (y_1, \dots, y_u)$  to stand for the variables appearing only in  $\phi$  and  $\mathbf{z} = (z_1, \dots, z_v)$  to stand for the variables appearing only in  $\psi$ , where  $d + u + v = n$ .

Since linear inequalities are trivially concave quadratic polynomials, our algorithm (Algorithm **IGFQC** in Section 4.4) can deal with the linear case too. In fact, it is a generalization of the algorithm for linear inequalities.

The proposed algorithm is recursive: the base case is when no sum of squares (SOS) polynomial can be generated by a nonpositive constant combination of nonstrict inequalities in  $\phi \wedge \psi$ . When this condition is not satisfied, i.e., an SOS polynomial can be generated by a nonpositive constant combination of nonstrict inequalities in  $\phi \wedge \psi$ , then it is possible to identify variables which can be eliminated by replacing them by linear expressions in terms of other variables and thus generate equisatisfiable problem with fewer variables on which the algorithm can be recursively invoked.

**Lemma 1.** *Let  $U \in \mathbb{R}^{(n+1) \times (n+1)}$  be a matrix. If  $\left\langle U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \leq 0$  for any  $\mathbf{x} \in \mathbb{R}^n$  and symmetric matrix  $\mathbf{X} \in \mathbb{R}^{n \times n}$  with  $\begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \succeq 0$ , then  $U \preceq 0$ .*

*Proof.* Assume that  $U \not\preceq 0$ . Then there exists a column vector  $\mathbf{y} = (y_0, y_1, \dots, y_n)^T \in \mathbb{R}^{n+1}$  such that  $c := \mathbf{y}^T U \mathbf{y} = \langle U, \mathbf{y} \mathbf{y}^T \rangle > 0$ . Denote  $M = \mathbf{y} \mathbf{y}^T$ , then  $M \succeq 0$ .

If  $y_0 \neq 0$ , then let  $\mathbf{x} = (\frac{y_1}{y_0}, \dots, \frac{y_n}{y_0})^T$ , and  $\mathbf{X} = \mathbf{x} \mathbf{x}^T$ . Thus,  $\begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x} \mathbf{x}^T \end{pmatrix} = \frac{1}{y_0^2} M \succeq 0$ , and  $\left\langle U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle = \left\langle U, \frac{1}{y_0^2} M \right\rangle = \frac{c}{y_0^2} > 0$ , which contradicts with  $\left\langle U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \leq 0$ .



If  $\mathbf{y}_0 = 0$ , then  $M_{(1,1)} = 0$ . Let  $M' = \frac{|U_{(1,1)}|+1}{c}M$ , then  $M' \succeq 0$ . Further, let  $M'' = M' + \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ . Then  $M'' \succeq 0$  and  $M''_{(1,1)} = 1$ . Let  $\begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} = M''$ , then

$$\begin{aligned} \left\langle U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle &= \langle U, M'' \rangle = \left\langle U, M' + \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \right\rangle \\ &= \left\langle U, \frac{|U_{(1,1)}|+1}{c}M + \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \right\rangle \\ &= \frac{|U_{(1,1)}|+1}{c} \langle U, M \rangle + U_{(1,1)} \\ &= |U_{(1,1)}| + 1 + U_{(1,1)} > 0, \end{aligned}$$

which also contradicts with  $\left\langle U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \leq 0$ . Thus, the assumption does not hold, that is  $U \preceq 0$ .  $\square$

**Lemma 2.** Let  $\mathcal{A} = \{\mathbf{y} \in \mathbb{R}^m \mid A_i \mathbf{y} - \alpha_i \geq 0, B_j \mathbf{y} - \beta_j > 0, \text{ for } i = 1, \dots, r, j = 1, \dots, \}$  be a nonempty set and  $\mathcal{B} \subseteq \mathbb{R}^m$  be a nonempty convex closed set. If  $\mathcal{A} \cap \mathcal{B} = \emptyset$  and there does not exist a linear form  $L(\mathbf{y})$  such that

$$\forall \mathbf{y} \in \mathcal{A}, L(\mathbf{y}) > 0, \text{ and } \forall \mathbf{y} \in \mathcal{B}, L(\mathbf{y}) \leq 0, \quad (5)$$

then there is a linear form  $L_0(\mathbf{y}) \not\equiv 0$  and  $\delta_1, \dots, \delta_r \geq 0$  such that

$$L_0(\mathbf{y}) = \sum_{i=1}^r \delta_i (A_i \mathbf{y} - \alpha_i) \text{ and } \forall \mathbf{y} \in \mathcal{B}, L_0(\mathbf{y}) \leq 0. \quad (6)$$

*Proof.* Since  $\mathcal{A}$  is defined by a set of linear inequalities,  $\mathcal{A}$  is a convex set. Using the separation theorem on disjoint convex sets, cf. e.g. [1], there exists a linear form  $L_0(\mathbf{y}) \not\equiv 0$  such that

$$\forall \mathbf{y} \in \mathcal{A}, L_0(\mathbf{y}) \geq 0, \text{ and } \forall \mathbf{y} \in \mathcal{B}, L_0(\mathbf{y}) \leq 0. \quad (7)$$

From (5) we have that

$$\exists \mathbf{y}_0 \in \mathcal{A}, L_0(\mathbf{y}_0) = 0. \quad (8)$$

Since

$$\forall \mathbf{y} \in \mathcal{A}, L_0(\mathbf{y}) \geq 0, \quad (9)$$

then

$$\begin{aligned} A_1 \mathbf{y} - \alpha_1 &\geq 0 \wedge \dots \wedge A_r \mathbf{y} - \alpha_r \geq 0 \wedge \\ B_1 \mathbf{y} - \beta_1 &> 0 \wedge \dots \wedge B_s \mathbf{y} - \beta_s > 0 \wedge -L_0(\mathbf{y}) > 0 \end{aligned}$$

has no solution w.r.t.  $\mathbf{y}$ . Using Corollary 1, there exist  $\lambda_1, \dots, \lambda_r \geq 0, \eta_0, \dots, \eta_s \geq 0$  and  $\eta \geq 0$  such that

$$\sum_{i=1}^r \lambda_i (A_i \mathbf{y} - \alpha_i) + \sum_{j=1}^s \eta_j (B_j \mathbf{y} - \beta_j) + \eta (-L_0(\mathbf{y})) + \eta_0 \equiv 0, \quad (10)$$

$$\sum_{j=0}^s \eta_j + \eta > 0. \quad (11)$$

Applying  $\mathbf{y}_0$  in (8) to (10) and (11), it follows

$$\eta_0 = \eta_1 = \dots = \eta_s = 0, \quad \eta > 0.$$

For  $i = 1, \dots, r$ , let  $\delta_i = \frac{\lambda_i}{\eta} \geq 0$ , then

$$L_0(\mathbf{y}) = \sum_{i=1}^r \delta_i (A_i \mathbf{y} - \alpha_i) \text{ and } \forall \mathbf{y} \in \mathcal{B}, L_0(\mathbf{y}) \leq 0. \quad \square$$

The lemma below asserts the existence of a strict linear inequality separating  $\mathcal{A}$  and  $\mathcal{B}$  defined above, for the case when any nonnegative constant combination of the linearization of  $f_i$ s is positive.

**Lemma 3.** *Let  $\mathcal{A} = \{\mathbf{y} \in \mathbb{R}^m \mid A_i \mathbf{y} - \alpha_i \geq 0, B_j \mathbf{y} - \beta_j > 0, \text{ for } i = 1, \dots, r, j = 1, \dots, s\}$  be a nonempty set and  $\mathcal{B} \subseteq \mathbb{R}^m$  be a nonempty convex closed set,  $\mathcal{A} \cap \mathcal{B} = \emptyset$ . There exists a linear form  $L(\mathbf{x}, \overline{\mathbf{X}})$  such that*

$$\forall (\mathbf{x}, \overline{\mathbf{X}}) \in \mathcal{A}, L(\mathbf{x}, \overline{\mathbf{X}}) > 0, \text{ and } \forall (\mathbf{x}, \overline{\mathbf{X}}) \in \mathcal{B}, L(\mathbf{x}, \overline{\mathbf{X}}) \leq 0,$$

whenever there does not exist  $\lambda_i \geq 0$ , s.t.,  $\sum_{i=1}^r \lambda_i P_i \preceq 0$ .

*Proof.* Proof is by contradiction. Given that  $\mathcal{A}$  is defined by a set of linear inequalities and  $\mathcal{B}$  is a closed convex nonempty set, by Lemma 2, there exist a linear form  $L_0(\mathbf{x}, \overline{\mathbf{X}}) \not\equiv 0$  and  $\delta_1, \dots, \delta_r \geq 0$  such that

$$L_0(\mathbf{x}, \overline{\mathbf{X}}) = \sum_{i=1}^r \delta_i \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \text{ and } \forall (\mathbf{x}, \overline{\mathbf{X}}) \in \mathcal{B}, L_0(\mathbf{x}, \overline{\mathbf{X}}) \leq 0.$$

I.e. there exists an symmetrical matrix  $\mathbf{L} \neq 0$  such that

$$\left\langle \mathbf{L}, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \equiv \sum_{i=1}^r \delta_i \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle, \quad (12)$$

$$\forall (\mathbf{x}, \overline{\mathbf{X}}) \in \mathcal{B}, \left\langle \mathbf{L}, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \leq 0. \quad (13)$$

Applying Lemma 1 to (13), it follows  $\mathbf{L} \preceq 0$ . This implies that  $\sum_{i=1}^r \delta_i P_i = \mathbf{L} \preceq 0$ , which is in contradiction to the assumption that there does not exist  $\lambda_i \geq 0$ , s.t.,  $\sum_{i=1}^r \lambda_i P_i \preceq 0$   $\square$

**Definition 5.** For given formulas  $\phi$  and  $\psi$  as in Problem 1, it satisfies the non-existence of an SOS condition (**NSOSC**) iff there do not exist  $\delta_1 \geq 0, \dots, \delta_r \geq 0$ , such that  $-(\delta_1 f_1 + \dots + \delta_r f_r)$  is a non-zero SOS.

The following theorem gives a method for generating an interpolant when the condition **NSOSC** holds by considering linearization of the problem and using Corollary 2. In that sense, this theorem is a generalization of Motzkin's theorem to CQ polynomial inequalities.

The following separation lemma about a nonempty convex set  $\mathcal{A}$  generated by linear inequalities that is disjoint from another nonempty closed convex set  $\mathcal{B}$  states that if there is no strict linear inequality that holds over  $\mathcal{A}$  and does not hold on any element in  $\mathcal{B}$ , then there is a hyperplane separating  $\mathcal{A}$  and  $\mathcal{B}$ , which is a nonnegative linear combination of nonstrict inequalities.

**Theorem 3.** Let  $f_1, \dots, f_r, g_1, \dots, g_s$  are CQ polynomials and the  $K$  is defined as in (3) with  $K = \emptyset$ . If the condition **NSOSC** holds, then there exist  $\lambda_i \geq 0$  ( $i = 1, \dots, r$ ),  $\eta_j \geq 0$  ( $j = 0, 1, \dots, s$ ) and a quadratic SOS polynomial  $h \in \mathbb{R}[\mathbf{x}]$  such that

$$\sum_{i=1}^r \lambda_i f_i + \sum_{j=1}^s \eta_j g_j + \eta_0 + h \equiv 0, \quad (14)$$

$$\eta_0 + \eta_1 + \dots + \eta_s = 1. \quad (15)$$

The proof uses the fact that if  $f_i$ s satisfy the **NSOSC** condition, then the linearization of  $f_i$ s and  $g_j$ s can be exploited to generate an interpolant expressed in terms of  $\mathbf{x}$ . The main issue is to decompose the result from the linearized problem into two components giving an interpolant.

*Proof.* Recall from Section 3.1 that

$$f_i = \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle, \quad g_j = \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle.$$

Let

$$\begin{aligned} \mathcal{A} &:= \{(\mathbf{x}, \overline{\mathbf{X}}) \mid \wedge_{i=1}^r \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle \geq 0, \wedge_{j=1}^s \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle > 0\}, \\ \mathcal{B} &:= \{(\mathbf{x}, \overline{\mathbf{X}}) \mid \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \succeq 0\}, \end{aligned} \quad (16)$$

be linearizations of the CQ polynomials  $f_i$ s and  $g_j$ s, where

$$\overline{\mathbf{X}} = (\mathbf{X}_{(1,1)}, \mathbf{X}_{(2,1)}, \mathbf{X}_{(2,2)}, \dots, \mathbf{X}_{(k,1)}, \dots, \mathbf{X}_{(k,k)}, \dots, \mathbf{X}_{(n,1)}, \dots, \mathbf{X}_{(n,n)}).$$

By Theorem 2,  $\mathcal{A} \cap \mathcal{B} = K_1 = K = \emptyset$ .

Since  $f_i$ s satisfy the **NSOSC** condition, its linearization satisfy the condition of Lemma 3; thus there exists a linear form  $\mathcal{L}(\mathbf{x}, \mathbf{X}) = \left\langle L, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle$  such that

$$\mathcal{L}(\mathbf{x}, \mathbf{X}) > 0, \text{ for } (\mathbf{x}, \mathbf{X}) \in \mathcal{A}, \quad (17)$$

$$\mathcal{L}(\mathbf{x}, \mathbf{X}) \leq 0, \text{ for } (\mathbf{x}, \mathbf{X}) \in \mathcal{B}. \quad (18)$$

Applying Lemma 1, it follows  $L \preceq 0$ . Additionally, applying Lemma 2 to (17) and denoting  $-L$  by  $P_0$ , there exist  $\bar{\lambda}_0, \bar{\lambda}_1, \dots, \bar{\lambda}_r \geq 0$  and  $\bar{\eta}_0, \bar{\eta}_1, \dots, \bar{\eta}_s \geq 0$  such that

$$\sum_{i=0}^r \bar{\lambda}_i \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \sum_{j=1}^s \bar{\eta}_j \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \bar{\eta}_0 \equiv 0, \\ \bar{\eta}_0 + \bar{\eta}_1 + \dots + \bar{\eta}_s > 0.$$

Let  $\lambda_i = \frac{\bar{\lambda}_i}{\sum_{j=0}^s \bar{\eta}_j}$ ,  $\eta_j = \frac{\bar{\eta}_j}{\sum_{j=0}^s \bar{\eta}_j}$ , then

$$\lambda_0 \left\langle -U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \sum_{i=1}^r \lambda_i \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \sum_{j=1}^s \eta_j \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{X} \end{pmatrix} \right\rangle + \eta_0 \equiv 0, \quad (19)$$

$$\eta_0 + \eta_1 + \dots + \eta_s = 1. \quad (20)$$

Since for any  $\mathbf{x}$  and symmetric matrix  $\mathbf{X}$ , (19) holds, by setting  $\mathbf{X} = \mathbf{x}\mathbf{x}^T$ ,

$$\lambda_0 \left\langle -U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle + \sum_{i=1}^r \lambda_i \left\langle P_i, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle + \sum_{j=1}^s \eta_j \left\langle Q_j, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle + \eta_0 \equiv 0,$$

which means that

$$h + \sum_{i=1}^r \lambda_i f_i + \sum_{j=1}^s \eta_j g_j + \eta_0 \equiv 0,$$

where  $h = \lambda_0 \left\langle -U, \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T \end{pmatrix} \right\rangle$ . Since  $U \preceq 0$ ,  $-U \succeq 0$ . Hence  $h$  is a quadratic SOS polynomial.  $\square$

#### 4.1 Base Case: Generating Interpolant when NSOSC is satisfied

Using the above theorem, it is possible to generate an interpolant for  $\phi$  and  $\psi$  from the SOS polynomial  $h$  obtained using the theorem which can be split into two SOS polynomials in the common variables of  $\phi$  and  $\psi$ . This is proved in the following theorem using some lemma as follows.

**Lemma 4.** *Given a quadratic SOS polynomial  $h(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbb{R}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$  on variables  $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{R}^d$ ,  $\mathbf{y} = (y_1, \dots, y_u) \in \mathbb{R}^u$  and  $\mathbf{z} = (z_1, \dots, z_v) \in \mathbb{R}^v$  such that the coefficients of  $y_i z_j$  ( $i = 1, \dots, u, j = 1, \dots, v$ ) are all vanished when expanding  $h(\mathbf{x}, \mathbf{y}, \mathbf{z})$ , there exist two quadratic polynomial  $h_1(\mathbf{x}, \mathbf{y}) \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2(\mathbf{x}, \mathbf{z}) \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  such that  $h = h_1 + h_2$ , moreover,  $h_1$  and  $h_2$  both are SOS.*

*Proof.* Since  $h(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is a quadratic polynomial and the coefficients of  $y_i z_j$  ( $i = 1, \dots, u, j = 1, \dots, v$ ) are all vanished when expanding  $h(\mathbf{x}, \mathbf{y}, \mathbf{z})$ , we have

$$h(\mathbf{x}, \mathbf{y}_1, \dots, \mathbf{y}_u, \mathbf{z}) = a_1 y_1^2 + b_1(\mathbf{x}, y_2, \dots, y_u) y_1 + c_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}),$$

where  $a_1 \in \mathbb{R}$ ,  $b_1(\mathbf{x}, y_2, \dots, y_u) \in \mathbb{R}[\mathbf{x}, y_2, \dots, y_u]$  is a linear function and  $c_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}) \in \mathbb{R}[\mathbf{x}, y_2, \dots, y_u, \mathbf{z}]$  is a quadratic polynomial. Since  $h(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is an SOS polynomial, so

$$\forall(\mathbf{x}, y_1, \dots, y_u, \mathbf{z}) \in \mathbb{R}^{d+u+v} \quad h(\mathbf{x}, y_1, \dots, y_u, \mathbf{z}) \geq 0.$$

Thus  $a_1 = 0 \wedge b_1 \equiv 0$  or  $a_1 > 0$ . If  $a_1 = 0 \wedge b_1 \equiv 0$  then we denote

$$p_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}) = c_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}), \quad q_1(\mathbf{x}, y_1, \dots, y_u) = 0;$$

otherwise,  $a_1 > 0$ , and we denote

$$p_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}) = h(\mathbf{x}, -\frac{b_1}{2a_1}, y_2, \dots, y_u, \mathbf{z}), \quad q_1(\mathbf{x}, y_1, \dots, y_u) = a_1(y_1 + \frac{b_1}{2a_1})^2.$$

Then, it is easy to see  $p_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z})$  is a quadratic polynomial satisfying

$$h(\mathbf{x}, y_1, \dots, y_u, \mathbf{z}) = p_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}) + q_1(\mathbf{x}, y_1, \dots, y_u),$$

and

$$\forall(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}) \in \mathbb{R}^{r+s-1+t} \quad p_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z}) \geq 0,$$

moreover, the coefficients of  $y_i z_j$  ( $i = 2, \dots, s, j = 1, \dots, t$ ) are all vanished when expanding  $p_1(\mathbf{x}, y_2, \dots, y_u, \mathbf{z})$ , and  $q_1(\mathbf{x}, y_1, \dots, y_u) \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  is an SOS. With the same reason, we can obtain  $p_2(\mathbf{x}, y_3, \dots, y_u, \mathbf{z}), \dots, p_u(\mathbf{x}, \mathbf{z})$  and  $q_2(\mathbf{x}, y_2, \dots, y_u), \dots, q_s(\mathbf{x}, y_u)$  such that

$$p_{i-1}(\mathbf{x}, y_i, \dots, y_u, \mathbf{z}) = p_i(\mathbf{x}, y_{i+1}, \dots, y_u, \mathbf{z}) + q_i(\mathbf{x}, y_i, \dots, y_u),$$

$$\forall(\mathbf{x}, y_{i+1}, \dots, y_u, \mathbf{z}) \in \mathbb{R}^{d+u-i+v} \quad p_i(\mathbf{x}, y_{i+1}, \dots, y_u, \mathbf{z}) \geq 0, \\ q_i(\mathbf{x}, y_i, \dots, y_u) \text{ is a SOS polynomial,}$$

for  $i = 2, \dots, u$ . Therefore, let

$$h_1(\mathbf{x}, \mathbf{y}) = q_1(\mathbf{x}, y_1, \dots, y_u) + \dots + q_s(\mathbf{x}, y_u), \quad h_2(\mathbf{x}, \mathbf{z}) = p_u(\mathbf{x}, \mathbf{z}),$$

we have  $h_1(\mathbf{x}, \mathbf{y}) \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  is an SOS and  $\forall(\mathbf{x}, \mathbf{z}) \in \mathbb{R}^{r+t} \quad h_2(\mathbf{x}, \mathbf{z}) = p_u(\mathbf{x}, \mathbf{z}) \geq 0$ . Hence,  $h_2(\mathbf{x}, \mathbf{z})$  is also an SOS, because that for the case of degree 2, a polynomial is positive semi-definite iff it is an SOS polynomial. Thus  $h_1(\mathbf{x}, \mathbf{y}) \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2(\mathbf{x}, \mathbf{z}) \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  are both SOS, moreover,

$$h_1 + h_2 = q_1 + \dots + q_{u-1} + q_u + p_u = q_1 + \dots + q_{u-1} + p_{u-1} = \dots = q_1 + p_1 = h. \quad \square$$

The above proof of Lemma 4 gives a method to express  $h, h_1, h_2$  as sums of squares of linear expressions and a nonnegative real number.

**Lemma 5.** Let  $h, h_1, h_2$  be as in the statement of Lemma 4. Then,

$$\begin{aligned} \text{(H)} : h(\mathbf{x}, \mathbf{y}, \mathbf{z}) = & a_1(y_1 - l_1(\mathbf{x}, y_2, \dots, y_u))^2 + \dots + a_u(y_u - l_u(\mathbf{x}))^2 + \\ & a_{u+1}(z_1 - l_{u+1}(\mathbf{x}, z_2, \dots, z_v))^2 + \dots + a_{u+v}(z_v - l_{u+v}(\mathbf{x}))^2 + \\ & a_{u+v+1}(x_1 - l_{u+v+1}(x_2, \dots, x_d))^2 + \dots + a_{u+v+d}(x_d - l_{u+v+d})^2 \\ & + a_{u+v+d+1}, \end{aligned}$$

where  $a_i \geq 0$  and  $l_j$  is a linear expression in the corresponding variables, for  $i = 1, \dots, u + v + d + 1, j = 1, \dots, u + v + d$ . Further,

$$\begin{aligned} \text{(H1)} : h_1(\mathbf{x}, \mathbf{y}) = & a_1(y_1 - l_1(\mathbf{x}, y_2, \dots, y_u))^2 + \dots + a_u(y_u - l_u(\mathbf{x}))^2 + \\ & \frac{a_{u+v+1}}{2}(x_1 - l_{u+v+1}(x_2, \dots, x_d))^2 + \dots + \frac{a_{u+v+d}}{2}(x_d - l_{u+v+d})^2 + \frac{a_{u+v+d+1}}{2}, \\ \text{(H2)} : h_2(\mathbf{x}, \mathbf{z}) = & a_{u+1}(z_1 - l_{u+1}(\mathbf{x}, z_2, \dots, z_v))^2 + \dots + a_{u+v}(z_v - l_{u+v}(\mathbf{x}))^2 + \\ & \frac{a_{u+v+1}}{2}(x_1 - l_{u+v+1}(x_2, \dots, x_d))^2 + \dots + \frac{a_{u+v+d}}{2}(x_d - l_{u+v+d})^2 + \frac{a_{u+v+d+1}}{2}. \end{aligned}$$

**Theorem 4.** Let  $\phi$  and  $\psi$  as defined in Problem 1 with  $\phi \wedge \psi \models \perp$ , which satisfy NSOSC. Then there exist  $\lambda_i \geq 0$  ( $i = 1, \dots, r$ ),  $\eta_j \geq 0$  ( $j = 0, 1, \dots, s$ ) and two quadratic SOS polynomial  $h_1 \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2 \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  such that

$$\sum_{i=1}^r \lambda_i f_i + \sum_{j=1}^s \eta_j g_j + \eta_0 + h_1 + h_2 \equiv 0, \quad (21)$$

$$\eta_0 + \eta_1 + \dots + \eta_s = 1. \quad (22)$$

Moreover, if  $\sum_{j=0}^{s_1} \eta_j > 0$ , then  $I > 0$  is an interpolant, otherwise  $I \geq 0$  is an interpolant, where  $I = \sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + h_1 \in \mathbb{R}[\mathbf{x}]$ .

*Proof.* From Theorem 3, there exist  $\lambda_i \geq 0$  ( $i = 1, \dots, r$ ),  $\eta_j \geq 0$  ( $j = 0, 1, \dots, s$ ) and a quadratic SOS polynomial  $h \in \mathbb{R}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$  such that

$$\sum_{i=1}^r \lambda_i f_i + \sum_{j=1}^s \eta_j g_j + \eta_0 + h \equiv 0, \quad (23)$$

$$\eta_0 + \eta_1 + \dots + \eta_s = 1. \quad (24)$$

Obviously, (23) is equivalent to the following formula

$$\sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + \sum_{i=r_1+1}^r \lambda_i f_i + \sum_{j=s_1+1}^s \eta_j g_j + h \equiv 0,$$

It's easy to see that

$$\sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 \in \mathbb{R}[\mathbf{x}, \mathbf{y}], \quad \sum_{i=r_1+1}^r \lambda_i f_i + \sum_{j=s_1+1}^s \eta_j g_j \in \mathbb{R}[\mathbf{x}, \mathbf{z}].$$

Thus, for any  $1 \leq i \leq u$ ,  $1 \leq j \leq v$ , the term  $\mathbf{y}_i \mathbf{z}_j$  does not appear in

$$\sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + \sum_{i=r_1+1}^r \lambda_i f_i + \sum_{j=s_1+1}^s \eta_j g_j.$$

Since all the conditions in Lemma 4 are satisfied, there exist two quadratic SOS polynomial  $h_1 \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2 \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  such that  $h = h_1 + h_2$ . Thus, we have

$$\begin{aligned} \sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + h_1 &\in \mathbb{R}[\mathbf{x}, \mathbf{y}], \\ \sum_{i=r_1+1}^r \lambda_i f_i + \sum_{j=s_1+1}^s \eta_j g_j + h_2 &\in \mathbb{R}[\mathbf{x}, \mathbf{z}], \\ \sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + h_1 + \sum_{i=r_1+1}^r \lambda_i f_i + \sum_{j=s_1+1}^s \eta_j g_j + h_2 &\equiv 0 \end{aligned}$$

Besides, as

$$I = \sum_{i=1}^{r_1} \lambda_i f_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + h_1 = -\left( \sum_{i=r_1+1}^r \lambda_i f_i + \sum_{j=s_1+1}^s \eta_j g_j + h_2 \right),$$

we have  $I \in \mathbb{R}[\mathbf{x}]$ . It is easy to see that

- if  $\sum_{j=0}^{s_1} \eta_j > 0$  then  $\phi \models I > 0$  and  $\psi \wedge I > 0 \models \perp$ , so  $I > 0$  is an interpolation;  
and
- if  $\sum_{j=s_1+1}^s \eta_j > 0$  then  $\phi \models I \geq 0$  and  $\psi \wedge I \geq 0 \models \perp$ , hence  $I \geq 0$  is an interpolation.  $\square$

## 4.2 Computing Interpolant using Semi-Definite Programming

Below, we formulate computing  $\lambda_i$ s,  $\eta_j$ s and  $h_1$  and  $h_2$  as a semi-definite programming problem.

Let

$$W = \begin{pmatrix} 1 & \mathbf{x}^T & \mathbf{y}^T & \mathbf{z}^T \\ \mathbf{x} & \mathbf{x}\mathbf{x}^T & \mathbf{x}\mathbf{y}^T & \mathbf{x}\mathbf{z}^T \\ \mathbf{y} & \mathbf{y}\mathbf{x}^T & \mathbf{y}\mathbf{y}^T & \mathbf{y}\mathbf{z}^T \\ \mathbf{z} & \mathbf{z}\mathbf{x}^T & \mathbf{z}\mathbf{y}^T & \mathbf{z}\mathbf{z}^T \end{pmatrix}$$

$$f_i = \langle P_i, W \rangle, \quad g_j = \langle Q_j, W \rangle, \quad (25)$$

where  $P_i$  and  $Q_j$  are  $(1 + d + u + v) \times (1 + d + u + v)$  matrices, and

$$h_1 = \langle M, W \rangle, \quad h_2 = \langle \hat{M}, W \rangle,$$

where  $M = (M_{ij})_{4 \times 4}$ ,  $\hat{M} = (\hat{M}_{ij})_{4 \times 4}$  with appropriate dimensions, for example  $M_{12} \in \mathbb{R}^{1 \times d}$  and  $\hat{M}_{34} \in \mathbb{R}^{u \times v}$ . Then, with NSOSC, by Theorem 4, Problem 1 is reduced to the following SDP feasibility problem.

**Find:**

$$\lambda_1, \dots, \lambda_r, \eta_0, \dots, \eta_s \in \mathbb{R} \text{ and real symmetric matrices}$$

$$M, \hat{M} \in \mathbb{R}^{(1+d+u+v) \times (1+d+u+v)}$$

subject to

$$\begin{cases} \sum_{i=1}^r \lambda_i P_i + \sum_{j=1}^s \eta_j Q_j + \eta_0 E_{1,1} + M + \hat{M} = 0, \sum_{j=0}^s \eta_j = 1, \\ M_{41} = (M_{14})^T = 0, M_{42} = (M_{24})^T = 0, M_{43} = (M_{34})^T = 0, M_{44} = 0, \\ \hat{M}_{31} = (\hat{M}_{13})^T = 0, \hat{M}_{32} = (\hat{M}_{23})^T = 0, \hat{M}_{33} = 0, \hat{M}_{34} = (\hat{M}_{43})^T = 0, \\ M \succeq 0, \hat{M} \succeq 0, \lambda_i \geq 0, \eta_j \geq 0, \text{ for } i = 1, \dots, r, j = 0, \dots, s, \end{cases}$$

where  $E_{1,1}$  is a  $(1+d+u+v) \times (1+d+u+v)$  matrix, whose  $(1,1)$  entry is 1 and the others are 0.

This is a standard **SDP** feasibility problem, which can be solved efficiently by well known **SDP** solvers, e.g., CSDP [3], SDPT3 [23], SeDuMi [19], etc., with time complexity polynomial in  $n = d + u + v$ .

*Remark 1.* Problem 1 is a typical quantifier elimination (QE) problem, which can be solved symbolically. However, it is very hard to solve large problems by general QE algorithms because of their high complexity. So, reducing Problem 1 to **SDP** problem makes it possible to solve many large problems in practice. Nevertheless, one may doubt whether we can use numerical result in verification. We think that verification must be rigorous and numerical results should be verified first. For example, after solving the above **SDP** problem numerically, we verify that whether  $-(\sum_{i=1}^r \lambda_i f_i + \sum_{j=1}^s \eta_j g_j + \eta_0)$  is an SOS by the method of Lemma 5, which is easy to do. If it is, the result is guaranteed and output. If not, the result is unknown (in fact, some other techniques can be employed in this case, which we do not discuss in this paper.). Thus, our algorithm is sound but not complete.

### 4.3 General Case

The case of  $\text{Var}(\phi) \subset \text{Var}(\psi)$  is not an issue since  $\phi$  serves as an interpolant of  $\phi$  and  $\psi$ . We thus assume that  $\text{Var}(\phi) \not\subseteq \text{Var}(\psi)$ . We show below how an interpolant can be generated in the general case. If  $\phi$  and  $\psi$  do not satisfy the **NSOSC** condition, i.e., an SOS polynomial  $h(\mathbf{x}, \mathbf{y}, \mathbf{z})$  can be computed from nonstrict inequalities  $f_i$ s using nonpositive constant multipliers, then by the lemma below, we can construct “simpler” interpolation subproblems  $\phi', \psi'$  from  $\phi$  and  $\psi$  by constructing from  $h$  an SOS polynomial  $f(\mathbf{x})$  such that  $\phi \models f(\mathbf{x}) \geq 0$  as well as  $\psi \models -f(\mathbf{x}) \geq 0$ . Each  $\phi', \psi'$  pair has the following characteristics because of which the algorithm is recursively applied to  $\phi'$  and  $\psi'$ .

- (i)  $\phi' \wedge \psi' \models \perp$ ,
- (ii)  $\phi', \psi'$  have the same form as  $\phi, \psi$ , i.e.,  $\phi'$  and  $\psi'$  are defined by some  $f'_i \geq 0$  and  $g'_j > 0$ , where  $f'_i$  and  $g'_j$  are CQ,
- (iii)  $\#(\text{Var}(\phi') \cup \text{Var}(\psi')) < \#(\text{Var}(\phi) \cup \text{Var}(\psi))$  to ensure termination of the recursive algorithm, and
- (iv) an interpolant  $I$  for  $\phi$  and  $\psi$  can be computed from an interpolant  $I'$  for  $\phi'$  and  $\psi'$  using  $f$ .



**Lemma 6.** *If Problem 1 does not satisfy the NSOSC condition, there exists  $f \in \mathbb{R}[\mathbf{x}]$ , such that  $\phi \Leftrightarrow \phi_1 \vee \phi_2$  and  $\psi \Leftrightarrow \psi_1 \vee \psi_2$ , where,*

$$\phi_1 = (f > 0 \wedge \phi), \quad \phi_2 = (f = 0 \wedge \phi), \quad (26)$$

$$\psi_1 = (-f > 0 \wedge \psi), \quad \psi_2 = (f = 0 \wedge \psi). \quad (27)$$

*Proof.* Since NSOSC does not hold, there exist  $\delta_1, \dots, \delta_r \in \mathbb{R}^+$  such that  $-\sum_{i=1}^r \delta_i f_i$  is a nonzero SOS. Let  $h(\mathbf{x}, \mathbf{y}, \mathbf{z})$  denote this quadratic SOS polynomial.

Since  $(-\sum_{i=1}^{r_1} \delta_i f_i) \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $(-\sum_{i=r_1+1}^r \delta_i f_i) \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$ , the coefficient of any term  $\mathbf{y}_i \mathbf{z}_j$ ,  $1 \leq i \leq u$ ,  $1 \leq j \leq v$ , is 0 after expanding  $h$ . By Lemma 4 there exist two quadratic SOS polynomials  $h_1 \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2 \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  such that  $h = h_1 + h_2$  with the following form:

$$(H1) : h_1(\mathbf{x}, \mathbf{y}) = a_1(\mathbf{y}_1 - l_1(\mathbf{x}, \mathbf{y}_2, \dots, \mathbf{y}_u))^2 + \dots + a_u(\mathbf{y}_u - l_u(\mathbf{x}))^2 + \frac{a_{u+v+1}}{2}(\mathbf{x}_1 - l_{u+v+1}(\mathbf{x}_2, \dots, \mathbf{x}_d))^2 + \dots + \frac{a_{u+v+d}}{2}(\mathbf{x}_d - l_{u+v+d})^2 + \frac{a_{u+v+d+1}}{2},$$

$$(H2) : h_2(\mathbf{x}, \mathbf{z}) = a_{u+1}(\mathbf{z}_1 - l_{u+1}(\mathbf{x}, \mathbf{z}_2, \dots, \mathbf{z}_v))^2 + \dots + a_{u+v}(\mathbf{z}_v - l_{u+v}(\mathbf{x}))^2 + \frac{a_{u+v+1}}{2}(\mathbf{x}_1 - l_{u+v+1}(\mathbf{x}_2, \dots, \mathbf{x}_d))^2 + \dots + \frac{a_{u+v+d}}{2}(\mathbf{x}_d - l_{u+v+d})^2 + \frac{a_{u+v+d+1}}{2}.$$

Let

$$f = \sum_{i=1}^{r_1} \delta_i f_i + h_1 = - \sum_{i=r_1+1}^r \delta_i f_i - h_2. \quad (28)$$

Obviously,  $f \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $f \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$ , this implies  $f \in \mathbb{R}[\mathbf{x}]$ .

Since  $h_1, h_2$  are SOS, it is easy to see that  $\phi \models f(\mathbf{x}) \geq 0$ ,  $\psi \models -f(\mathbf{x}) \geq 0$ . Thus,  $\phi \Leftrightarrow \phi_1 \vee \phi_2$ ,  $\psi \Leftrightarrow \psi_1 \vee \psi_2$ .  $\square$

Using the above lemma, an interpolant  $I$  for  $\phi$  and  $\psi$  can be constructed from an interpolant  $I_{2,2}$  for  $\phi_2$  and  $\psi_2$ .

**Theorem 5.** *Let  $\phi, \psi, \phi_1, \phi_2, \psi_1, \psi_2$  as defined in Lemma 6, then given an interpolant  $I_{2,2}$  for  $\phi_2$  and  $\psi_2$ ,  $I := (f > 0) \vee (f \geq 0 \wedge I_{2,2})$  is an interpolant for  $\phi$  and  $\psi$ .*

*Proof.* It is easy to see that  $f > 0$  is an interpolant for both  $(\phi_1, \psi_1)$  and  $(\phi_1, \psi_2)$ , and  $f \geq 0$  is an interpolant for  $(\phi_2, \psi_1)$ . Thus, if  $I_{2,2}$  is an interpolant for  $(\phi_2, \psi_2)$ , then  $I$  is an interpolant for  $\phi$  and  $\psi$ .  $\square$

An interpolant for  $\phi_2$  and  $\psi_2$  is constructed recursively since the new constraint included in  $\phi_2$  (similarly, as well as in  $\psi_2$ ) is:  $\sum_{i=1}^{r_1} \delta_i f_i + h_1 = 0$  with  $h_1$  being an SOS. Let  $\phi'$  and  $\psi'$  stand for the formulas constructed after analyzing  $\phi_2$  and  $\psi_2$  respectively. Given that  $\delta_i$  as well as  $f_i \geq 0$  for each  $i$ , case analysis is performed on  $h_1$  depending upon whether it has a positive constant  $a_{u+v+d+1} > 0$  or not.

**Theorem 6.** *Let  $\phi' \triangleq (0 > 0)$  and  $\psi' \triangleq (0 > 0)$ . In the proof of Lemma 6, if  $a_{u+v+d+1} > 0$ , then  $\phi'$  and  $\psi'$  satisfy (i) – (iv).*

*Proof.* (i), (ii) and (iii) are trivially satisfied. Since  $a_{u+v+d+1} > 0$ , it is easy to see that  $h_1 > 0$  and  $h_2 > 0$ . From (26), (27) and (28), we have  $\phi_2 \models h_1 = 0$ , and  $\psi_2 \models h_2 = 0$ . Thus  $\phi_2 \Leftrightarrow \phi' \Leftrightarrow \perp$  and  $\psi_2 \Leftrightarrow \psi' \Leftrightarrow \perp$ .  $\square$

In case  $a_{u+v+d+1} = 0$ , from the fact that  $h_1$  is an SOS and has the form (H1), each nonzero square term in  $h_1$  is identically 0. This implies that some of the variables in  $\mathbf{x}, \mathbf{y}$  can be linearly expressed in term of other variables; the same argument applies to  $h_2$  as well. In particular, at least one variable is eliminated in both  $\phi_2$  and  $\psi_2$ , reducing the number of variables appearing in  $\phi$  and  $\psi$ , which ensures the termination of the algorithm. A detailed analysis is given in following lemmas, where it is shown how this elimination of variables is performed, generating  $\phi'$  and  $\psi'$  on which the algorithm can be recursively invoked; an a theorem is also proved to ensures this.

**Lemma 7.** *In the proof of Lemma 6, if  $a_{u+v+d+1} = 0$ , then  $\mathbf{x}$  can be represented as  $(\mathbf{x}^1, \mathbf{x}^2)$ ,  $\mathbf{y}$  as  $(\mathbf{y}^1, \mathbf{y}^2)$  and  $\mathbf{z}$  as  $(\mathbf{z}^1, \mathbf{z}^2)$ , such that*

$$\begin{aligned}\phi_2 &\models ((\mathbf{y}^1 = \Lambda_1 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{y}^2 \end{pmatrix} + \gamma_1) \wedge (\mathbf{x}^1 = \Lambda_3 \mathbf{x}^2 + \gamma_3)), \\ \psi_2 &\models ((\mathbf{z}^1 = \Lambda_2 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{z}^2 \end{pmatrix} + \gamma_2) \wedge (\mathbf{x}^1 = \Lambda_3 \mathbf{x}^2 + \gamma_3)),\end{aligned}$$

and  $\#(\text{Var}(\mathbf{x}^1) + \text{Var}(\mathbf{y}^1) + \text{Var}(\mathbf{z}^1)) > 0$ , for matrixes  $\Lambda_1, \Lambda_2, \Lambda_3$  and vectors  $\gamma_1, \gamma_2, \gamma_3$ .

*Proof.* From (26), (27) and (28) we have

$$\phi_2 \models h_1 = 0, \quad \psi_2 \models h_2 = 0. \quad (29)$$

Since  $h_1 + h_2 = h$  is a nonzero polynomial,  $a_{u+v+d+1} = 0$ , then there exist some  $a_i \neq 0$ , i.e.  $a_i > 0$ , for  $1 \leq i \leq u + v + d$ . Let

$$\begin{aligned}N_1 &:= \{i \mid a_i > 0 \wedge 1 \leq i \leq u\}, \\ N_2 &:= \{i \mid a_{u+i} > 0 \wedge 1 \leq i \leq v\}, \\ N_3 &:= \{i \mid a_{u+v+i} > 0 \wedge 1 \leq i \leq d\}.\end{aligned}$$

Thus,  $N_1, N_2$  and  $N_3$  cannot all be empty. In addition,  $h_1 = 0$  implies that

$$\begin{aligned}\mathbf{y}_i &= l_i(\mathbf{x}, \mathbf{y}_{i+1}, \dots, \mathbf{y}_u), \quad \text{for } i \in N_1, \\ \mathbf{x}_i &= l_{u+v+i}(\mathbf{x}_{i+1}, \dots, \mathbf{z}_d), \quad \text{for } i \in N_3.\end{aligned}$$

Also,  $h_2 = 0$  implies that

$$\begin{aligned}\mathbf{z}_i &= l_{u+i}(\mathbf{x}, \mathbf{z}_{i+1}, \dots, \mathbf{z}_v), \quad \text{for } i \in N_2, \\ \mathbf{x}_i &= l_{u+v+i}(\mathbf{x}_{i+1}, \dots, \mathbf{z}_d), \quad \text{for } i \in N_3.\end{aligned}$$

Now, let

$$\begin{aligned}
\mathbf{y}^1 &= (y_{i_1}, \dots, y_{i_{|N_1|}}), \mathbf{y}^2 = (y_{j_1}, \dots, y_{j_{u-|N_1|}}), \\
&\text{where } \{i_1, \dots, i_{|N_1|}\} = N_1, \{j_1, \dots, j_{u-|N_1|}\} = \{1, \dots, u\} - N_1, \\
\mathbf{z}^1 &= (z_{i_1}, \dots, z_{i_{|N_2|}}), \mathbf{z}^2 = (z_{j_1}, \dots, z_{j_{v-|N_2|}}), \\
&\text{where } \{i_1, \dots, i_{|N_2|}\} = N_2, \{j_1, \dots, j_{v-|N_2|}\} = \{1, \dots, v\} - N_2, \\
\mathbf{x}^1 &= (x_{i_1}, \dots, x_{i_{|N_3|}}), \mathbf{x}^2 = (x_{j_1}, \dots, x_{j_{d-|N_3|}}), \\
&\text{where } \{i_1, \dots, i_{|N_3|}\} = N_3, \{j_1, \dots, j_{d-|N_3|}\} = \{1, \dots, d\} - N_3.
\end{aligned}$$

Clearly,  $\#(\text{Var}(\mathbf{x}^1) + \text{Var}(\mathbf{y}^1) + \text{Var}(\mathbf{z}^1)) > 0$ . By linear algebra, there exist three matrices  $\Lambda_1, \Lambda_2, \Lambda_3$  and three vectors  $\gamma_1, \gamma_2, \gamma_3$  s.t.

$$\begin{aligned}
\mathbf{y}^1 &= \Lambda_1 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{y}^2 \end{pmatrix} + \gamma_1, \\
\mathbf{z}^1 &= \Lambda_2 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{z}^2 \end{pmatrix} + \gamma_2, \\
\mathbf{x}^1 &= \Lambda_3 \mathbf{x}^2 + \gamma_3.
\end{aligned}$$

Since  $\phi_2 \models h_1 = 0, \quad \psi_2 \models h_2 = 0$ , then,

$$\begin{aligned}
\phi_2 &\models ((\mathbf{y}^1 = \Lambda_1 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{y}^2 \end{pmatrix} + \gamma_1) \wedge (\mathbf{x}^1 = \Lambda_3 \mathbf{x}^2 + \gamma_3)), \\
\psi_2 &\models ((\mathbf{z}^1 = \Lambda_2 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{z}^2 \end{pmatrix} + \gamma_2) \wedge (\mathbf{x}^1 = \Lambda_3 \mathbf{x}^2 + \gamma_3)).
\end{aligned}$$

□

So, replacing  $(\mathbf{x}^1, \mathbf{y}^1)$  in  $f_i(\mathbf{x}, \mathbf{y})$  and  $g_j(\mathbf{x}, \mathbf{y})$  by  $\Lambda_3 \mathbf{x}^2 + \gamma_3 \quad \Lambda_1 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{y}^2 \end{pmatrix} + \gamma_1$  respectively, results in new polynomials  $\hat{f}_i(\mathbf{x}^2, \mathbf{y}^2)$  and  $\hat{g}_j(\mathbf{x}^2, \mathbf{y}^2)$ , for  $i = 1, \dots, r_1, j = 1, \dots, s_1$ . Similarly, replacing  $(\mathbf{x}^1, \mathbf{z}^1)$  in  $f_i(\mathbf{x}, \mathbf{z})$  and  $g_j(\mathbf{x}, \mathbf{z})$  by  $\Lambda_3 \mathbf{x}^2 + \gamma_3$  and  $\Lambda_2 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{z}^2 \end{pmatrix} + \gamma_2$  respectively, derives new polynomials  $\hat{f}_i(\mathbf{x}^2, \mathbf{z}^2)$  and  $\hat{g}_j(\mathbf{x}^2, \mathbf{z}^2)$ , for  $i = r_1 + 1, \dots, r, j = s_1 + 1, \dots, s$ . Regarding the resulted polynomials above, we have the following property.

**Lemma 8.** Let  $\xi \in \mathbb{R}^m$  and  $\zeta \in \mathbb{R}^n$  be two vector variables,  $g(\xi, \zeta) = \begin{pmatrix} \xi \\ \zeta \end{pmatrix}^T G \begin{pmatrix} \xi \\ \zeta \end{pmatrix} + a^T \begin{pmatrix} \xi \\ \zeta \end{pmatrix} + \alpha$  be a CQ polynomial on  $(\xi, \zeta)$ , i.e.  $G \preceq 0$ . Replacing  $\zeta$  in  $g$  by  $\Lambda \xi + \gamma$  derives  $\hat{g}(\xi) = g(\xi, \Lambda \xi + \gamma)$ , then  $\hat{g}(\xi)$  is a CQ polynomial in  $\xi$ .

*Proof.*  $G \preceq 0$  iff  $-\begin{pmatrix} \xi \\ \zeta \end{pmatrix}^T G \begin{pmatrix} \xi \\ \zeta \end{pmatrix}$  is an SOS. Thus, there exist  $l_{i,1} \in \mathbb{R}^m, l_{i,2} \in \mathbb{R}^n$ , for  $i = 1, \dots, s, s \in \mathbb{N}^+$  s.t.  $\begin{pmatrix} \xi \\ \zeta \end{pmatrix}^T G \begin{pmatrix} \xi \\ \zeta \end{pmatrix} = -\sum_{i=1}^s (l_{i,1}^T \xi + l_{i,2}^T \zeta)^2$ . Hence,

$$\begin{aligned} \begin{pmatrix} \xi \\ \Lambda \xi + \gamma \end{pmatrix}^T G \begin{pmatrix} \xi \\ \Lambda \xi + \gamma \end{pmatrix} &= -\sum_{i=1}^s (l_{i,1}^T \xi + l_{i,2}^T (\Lambda \xi + \gamma))^2 \\ &= -\sum_{i=1}^s ((l_{i,1}^T + l_{i,2}^T \Lambda) \xi + l_{i,2}^T \gamma)^2 \\ &= -\sum_{i=1}^s ((l_{i,1}^T + l_{i,2}^T \Lambda) \xi)^2 + l(\xi), \end{aligned}$$

where  $l(\xi)$  is a linear function in  $\xi$ . Then we have

$$\hat{g}(\xi) = -\sum_{i=1}^s ((l_{i,1}^T + l_{i,2}^T \Lambda) \xi)^2 + l(\xi) + \alpha^T \begin{pmatrix} \xi \\ \Lambda \xi + \gamma \end{pmatrix} + \alpha.$$

Obviously, there exist  $\hat{G} \preceq 0, \hat{\alpha}$  and  $\hat{\alpha}$  such that

$$\hat{g} = \xi \hat{G} \xi^T + \hat{\alpha}^T \xi + \hat{\alpha}.$$

Therefore,  $\hat{g}$  is concave quadratic polynomial in  $\xi$ . □

**Theorem 7.** *In the proof of Lemma 6, if  $a_{u+v+d+1} = 0$ , then Lemma 7 holds. So, let  $\hat{f}_i$  and  $\hat{g}_j$  as above, and*

$$\begin{aligned} \phi' &= \bigwedge_{i=1}^{r_1} \hat{f}_i \geq 0 \wedge \bigwedge_{j=1}^{s_1} \hat{g}_j > 0, \\ \psi' &= \bigwedge_{i=r_1+1}^r \hat{f}_i \geq 0 \wedge \bigwedge_{j=s_1+1}^s \hat{g}_j > 0. \end{aligned}$$

Then  $\phi'$  and  $\psi'$  satisfy (i) – (iv).

*Proof.* From Lemma 7, we have

$$\begin{aligned} \phi_2 &\models ((\mathbf{y}^1 = \Lambda_1 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{y}^2 \end{pmatrix} + \gamma_1) \wedge (\mathbf{x}^1 = \Lambda_3 \mathbf{x}^2 + \gamma_3)), \\ \psi_2 &\models ((\mathbf{z}^1 = \Lambda_2 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{z}^2 \end{pmatrix} + \gamma_2) \wedge (\mathbf{x}^1 = \Lambda_3 \mathbf{x}^2 + \gamma_3)). \end{aligned}$$

Let

$$\begin{aligned}\phi'_2 &:= ((\mathbf{y}^1 = A_1 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{y}^2 \end{pmatrix} + \gamma_1) \wedge (\mathbf{x}^1 = A_3 \mathbf{x}^2 + \gamma_3) \wedge \phi), \\ \psi'_2 &:= ((\mathbf{z}^1 = A_2 \begin{pmatrix} \mathbf{x}^2 \\ \mathbf{z}^2 \end{pmatrix} + \gamma_2) \wedge (\mathbf{x}^1 = A_3 \mathbf{x}^2 + \gamma_3) \wedge \psi).\end{aligned}$$

Then  $\phi_2 \models \phi'_2$ ,  $\phi_2 \models \psi'_2$  and  $\phi'_2 \wedge \psi'_2 \models \perp$ . Thus any interpolant for  $\phi'_2$  and  $\psi'_2$  is also an interpolant of  $\phi_2$  and  $\psi_2$ .

By the definition of  $\phi'$  and  $\psi'$ , it follows  $\phi' \wedge \psi' \models \perp$  iff  $\phi'_2 \wedge \psi'_2 \models \perp$ , so  $\phi' \wedge \psi' \models \perp$ , (i) holds.

Moreover,  $\phi_2' \models \phi'$ ,  $\psi_2' \models \psi'$ ,  $\text{Var}(\phi') \subseteq \text{Var}(\phi_2')$  and  $\text{Var}(\psi') \subseteq \text{Var}(\psi_2')$ , then any interpolant for  $\phi'$  and  $\psi'$  is also an interpolant for  $\phi_2'$  and  $\psi_2'$ , then also an interpolant for  $\phi_2$  and  $\psi_2$ . By Theorem 5, (iii) holds.

Since  $\#(\text{Var}(\phi) + \text{Var}(\psi)) - \#(\text{Var}(\phi') + \text{Var}(\psi')) = \#(\mathbf{x}^1, \mathbf{y}^1, \mathbf{z}^1) > 0$ , then (vi) holds.

For (ii),  $\phi', \psi'$  have the same form with  $\phi, \psi$ , means that  $\hat{f}_i, i = 1, \dots, r$  are CQ and  $\hat{g}_j, j = 1, \dots, s$  are CQ. This is satisfied directly by Lemma 8.  $\square$

The following simple example illustrates how the above construction works.

*Example 2.* Let  $f_1 = x_1, f_2 = x_2, f_3 = -x_1^2 - x_2^2 - 2x_2 - z^2, g_1 = -x_1^2 + 2x_1 - x_2^2 + 2x_2 - y^2$ . Two formulas  $\phi := (f_1 \geq 0) \wedge (f_2 \geq 0) \wedge (g_1 > 0), \psi := (f_3 \geq 0)$ .  $\phi \wedge \psi \models \perp$ .

The condition NSOSC does not hold, since

$$-(0f_1 + 2f_2 + f_3) = x_1^2 + x_2^2 + z^2 \text{ is a sum of square.}$$

Then we have  $h = x_1^2 + x_2^2 + z^2$ , and

$$h_1 = \frac{1}{2}x_1^2 + \frac{1}{2}x_2^2, \quad h_2 = \frac{1}{2}x_1^2 + \frac{1}{2}x_2^2 + z^2. \quad (30)$$

Let  $f = 0f_1 + 2f_2 + h_1 = \frac{1}{2}x_1^2 + \frac{1}{2}x_2^2 + 2x_2$ .

For the recursive call, we have  $f = 0$  as well as  $x_1 = 0, x_2 = 0$  from  $h_1 = 0$  to construct  $\phi'$  from  $\phi$ ; similarly  $\psi'$  is constructing by setting  $x_1 = x_2 = 0, z = 0$  in  $\psi$  as derived from  $h_2 = 0$ .

$$\phi' = 0 \geq 0 \wedge 0 \geq 0 \wedge -y^2 > 0 = \perp, \quad \psi' = 0 \geq 0 = \top.$$

Thus,  $I(\phi', \psi') := (0 > 0)$  is an interpolant for  $(\phi', \psi')$ .

An interpolant for  $\phi$  and  $\psi$  is thus  $(f(x) > 0) \vee (f(x) = 0 \wedge I(\phi', \psi'))$ , which is  $\frac{1}{2}x_1^2 + \frac{1}{2}x_2^2 + 2x_2 > 0$ .

---

**Algorithm 1: IGFCH**


---

**input** : Two formulas  $\phi, \psi$  with **NSOSC** and  $\phi \wedge \psi \models \perp$ , where  
 $\phi = f_1 \geq 0 \wedge \dots \wedge f_{r_1} \geq 0 \wedge g_1 > 0 \wedge \dots \wedge g_{s_1} > 0$ ,  
 $\psi = f_{r_1+1} \geq 0 \wedge \dots \wedge f_r \geq 0 \wedge g_{s_1+1} > 0 \wedge \dots \wedge g_s > 0$ ,  
 $f_1, \dots, f_r, g_1, \dots, g_s$  are all concave quadratic polynomials,  
 $f_1, \dots, f_{r_1}, g_1, \dots, g_{s_1} \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$ ,  $f_{r_1+1}, \dots, f_r, g_{s_1+1}, \dots, g_s \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$   
**output**: A formula  $I$  to be a Craig interpolant for  $\phi$  and  $\psi$   
**1 Find**  $\lambda_1, \dots, \lambda_r \geq 0, \eta_0, \eta_1, \dots, \eta_s \geq 0, h_1 \in \mathbb{R}[\mathbf{x}, \mathbf{y}], h_2 \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  by SDP s.t.

$$\sum_{i=1}^r \lambda_i g_i + \sum_{j=1}^s \eta_j g_j + \eta_0 + h_1 + h_2 \equiv 0,$$

$$\eta_0 + \eta_1 + \dots + \eta_s = 1,$$

$$h_1, h_2 \text{ are SOS polynomial};$$

/\* This is essentially a **SDP** problem, see Section 4.1 \*/  
**2**  $f := \sum_{i=1}^{r_1} \lambda_i g_i + \sum_{j=1}^{s_1} \eta_j g_j + \eta_0 + h_1$ ;  
**3 if**  $\sum_{j=0}^{s_1} \eta_j > 0$  **then**  $I := (f > 0)$ ; **else**  $I := (f \geq 0)$ ;  
**4 return**  $I$

---

#### 4.4 Algorithms

Algorithm **IGFCH** deals with the case when  $\phi$  and  $\psi$  satisfy the **NSOSC** condition.

**Theorem 8 (Soundness and Completeness of IGFCH).** *IGFCH computes an interpolant  $I$  of mutually contradictory  $\phi, \psi$  with CQ polynomial inequalities satisfying the NSOSC condition.*

*Proof.* It is guaranteed by Theorem 4. □

The recursive algorithm **IGFCH** is given below. For the base case when  $\phi, \psi$  satisfy the **NSOSC** condition, it invokes **IGFCH**.

**Theorem 9 (Soundness and Completeness of IGFQC).** *IGFQC computes an interpolant  $I$  of mutually contradictory  $\phi, \psi$  with CQ polynomial inequalities.*

*Proof.* If  $\text{Var}(\phi) \subseteq \text{Var}(\psi)$ , **IGFQC** terminates at step 1, and returns  $\phi$  as an interpolant. Otherwise, there are two cases:

(i) If **NSOSC** holds, then **IGFQC** terminates at step 3 and returns an interpolant for  $\phi$  and  $\psi$  by calling **IGFCH**. Its soundness and completeness follows from the previous theorem.

(ii)  $\text{Var}(\phi) \not\subseteq \text{Var}(\psi)$  and **NSOSC** does not hold: The proof is by induction on the number of recursive calls to **IGFQC**, with the case of 0 recursive calls being (i) above.

In the induction step, assume that for a  $k^{\text{th}}$ -recursive call to **IGFQC** gives a correct interpolant  $I'$  for  $\phi'$  and  $\psi'$ , where  $\phi'$  and  $\psi'$  are constructed by Theorem 6 or Theorem 7.

---

**Algorithm 2: IGFQC**


---

**input** : Two formulas  $\phi, \psi$  with  $\phi \wedge \psi \models \perp$ , where  
 $\phi = f_1 \geq 0 \wedge \dots \wedge f_{r_1} \geq 0 \wedge g_1 > 0 \wedge \dots \wedge g_{s_1} > 0$ ,  
 $\psi = f_{r_1+1} \geq 0 \wedge \dots \wedge f_r \geq 0 \wedge g_{s_1+1} > 0 \wedge \dots \wedge g_s > 0$ ,  
 $f_1, \dots, f_r, g_1, \dots, g_s$  are all CQ polynomials,  
 $f_1, \dots, f_{r_1}, g_1, \dots, g_{s_1} \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$ , and  $f_{r_1+1}, \dots, f_r, g_{s_1+1}, \dots, g_s \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$

**output**: A formula  $I$  to be a Craig interpolant for  $\phi$  and  $\psi$

- 1 **if**  $\text{Var}(\phi) \subseteq \text{Var}(\psi)$  **then**  $I := \phi$ ; **return**  $I$ ;
- 2 **Find**  $\delta_1, \dots, \delta_r \geq 0, h \in \mathbb{R}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$  by SDP s.t.  $\sum_{i=1}^r \delta_i f_i + h \equiv 0$  and  $h$  is SOS;  
/\* Check the condition **NSOSC** \*/
- 3 **if no solution** **then**  $I := \text{IGFCH}(\phi, \psi)$ ; **return**  $I$ ;  
/\* **NSOSC** holds \*/
- 4 Construct  $h_1 \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2 \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  with the forms (H1) and (H2);
- 5  $f := \sum_{i=1}^{r_1} \delta_i f_i + h_1 = -\sum_{i=r_1+1}^r \delta_i f_i - h_2$ ;
- 6 Construct  $\phi'$  and  $\psi'$  using Theorem 6 and Theorem 7 by eliminating variables due to  
 $h_1 = h_2 = 0$ ;
- 7  $I' = \text{IGFQC}(\phi', \psi')$ ;
- 8  $I := (f > 0) \vee (f \geq 0 \wedge I')$ ;
- 9 **return**  $I$

---

By Theorem 7, the interpolant  $I$  constructed from  $I'$  is the correct answer for  $\phi$  and  $\psi$ .

The recursive algorithm terminates in all three cases: (i)  $\text{Var}(\phi) \subseteq \text{Var}(\psi)$ , (ii) **NSOSC** holds, which is achieved at most  $u + v + d$  times by Theorem 7, and (iii) the number of variables in  $\phi', \psi'$  in the recursive call is smaller than the number of variables in  $\phi, \psi$ . □

#### 4.5 Complexity analysis of IGFCH and IGFQC

It is well known that an **SDP** problem can be solved in polynomial time complexity. We analyze the complexity of the above algorithms assuming that the complexity of an **SDP** problem is of time complexity  $g(k)$ , where  $k$  is the input size.

**Theorem 10.** *The complexity of IGFCH is  $\mathcal{O}(g(r + s + n^2))$ , where  $r$  is the number of nonstrict inequalities  $f_i$ s and  $s$  is the number of strict inequalities  $g_j$ s, and  $n$  is the number of variables in  $f_i$ s and  $g_j$ s.*

*Proof.* In this algorithm we first need to solve a constraint solving problem in step 1, see Section 4.1, it is an **SDP** problem with size  $\mathcal{O}(r + s + n^2)$ , so the complexity of step 1 is  $\mathcal{O}(g(r + s + n^2))$ . Obviously, the complexity of steps 2 – 4 is linear in  $(r + s + n^2)$ , so the complexity of **IGFCH** is  $\mathcal{O}(g(r + s + n^2))$ . □

**Theorem 11.** *The complexity of IGFQC is  $\mathcal{O}(n * g(r + s + n^2))$ , where  $r, s, n$  are as defined in the previous theorem.*

*Proof.* The algorithm **IGFQC** is a recursive algorithm, which is called at most  $n$  times, since in every recursive call, at least one variable gets eliminated. Finally, it terminates at step 1 or step 3 with complexity  $\mathcal{O}(g(r + s + n^2))$ .

The complexity of each recursive call, i.e., the complexity for step 2 and steps 4 – 9, can be analyzed as follows:

For step 2, checking if **NSOSC** holds is done by solving the following problem:

**find:**  $\delta_1, \dots, \delta_r \geq 0$ , and an SOS polynomial  $h \in \mathbb{R}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$  s.t.  $\sum_{i=1}^r \delta_i f_i + h \equiv 0$ , which is equivalent to the following linear matrix inequality (**LM**),

**find:**  $\delta_1, \dots, \delta_r \geq 0$ ,  $M \in R^{(n+1) \times (n+1)}$ , s.t.  $M = -\sum_{i=1}^r \delta_i P_i$ ,  $M \succeq 0$ , where  $P_i \in R^{(n+1) \times (n+1)}$  is defined as (25). Clearly, this is an **SDP** problem with size  $\mathcal{O}(r + n^2)$ , so the complexity of this step is  $\mathcal{O}(g(r + n^2))$ .

For steps 4 – 9, by the proof of Lemma 4, it is easy to see that to represent  $h$  in the form (H) in Lemma 5 can be done with complexity  $\mathcal{O}(n^2)$ ,  $h_1$  and  $h_2$  can be computed with complexity  $\mathcal{O}(n^2)$ . Thus, the complexity of step 4 is  $\mathcal{O}(n^2)$ . Step 5 is much easy. For step 6, using linear algebra operations, it is easy to see that the complexity is  $\mathcal{O}(n^2 + r + s)$ . So, the complexity is  $\mathcal{O}(n^2 + r + s)$  for step 4 – 9.

In a word, the overall complexity of **IGFQC** is

$$\mathcal{O}(g(r + s + n^2)) + n\mathcal{O}(n^2 + r + s) = \mathcal{O}(n * g(r + s + n^2)).$$

□

## 5 Combination: quadratic concave polynomial inequalities with uninterpreted function symbols (*EUF*)

This section combines the quantifier-free theory of quadratic concave polynomial inequalities with the theory of equality over uninterpreted function symbols (*EUF*). The proposed algorithm for generating interpolants for the combined theories is presented in Algorithm 6. As the reader would observe, it is patterned after the algorithm  $\text{INTER}_{LI(Q)^S}$  in Figure 4 in [17] following the hierarchical reasoning and interpolation generation framework in [21] with the following key differences<sup>6</sup>:

1. To generate interpolants for mutually contradictory conjunctions of CQ polynomial inequalities, we call **IGFQC**.
2. We prove below that (i) a nonlinear equality over polynomials cannot be generated from CQ polynomials, and furthermore (ii) in the base case when the **NSOSC** condition is satisfied by CQ polynomial inequalities, linear equalities are deduced only from the linear inequalities in a problem (i.e., nonlinear inequalities do not play any role); separating terms for mixed equalities are computed the same way as in the algorithm SEP in [17], and (iii) as shown in Lemmas 4, 5 and Theorem 7, during recursive calls to **IGFQC**, additional linear unmixed equalities are deduced which are local to either  $\phi$  or  $\psi$ , we can use these equalities as well as those in (ii) for the base case to reduce the number of variables appearing in  $\phi$  and  $\psi$  thus reducing the complexity of the algorithm; equalities relating variables of  $\phi$  are also included in the interpolant.

<sup>6</sup> The proposed algorithm and its way of handling of combined theories do not crucially depend upon using algorithms in [17]; however, adopting their approach makes proofs and presentation easier by focusing totally on the quantifier-free theory of CQ polynomial inequalities.



Other than that, the proposed algorithm reduces to  $\text{INTER}_{LI(Q)^{\exists}}$  if  $\phi, \psi$  are purely from  $LI(Q)$  and/or  $EUF$ .

In order to get directly to the key concepts used, we assume the reader's familiarity with the basic construction of flattening and purification by introducing fresh variables for the arguments containing uninterpreted functions.

### 5.1 Problem Formulation

Let  $\Omega = \Omega_1 \cup \Omega_2 \cup \Omega_3$  be a finite set of uninterpreted function symbols in  $EUF$ ; further, denote  $\Omega_1 \cup \Omega_2$  by  $\Omega_{12}$  and  $\Omega_1 \cup \Omega_3$  by  $\Omega_{13}$ . Let  $\mathbb{R}[\mathbf{x}, \mathbf{y}, \mathbf{z}]^{\Omega}$  be the extension of  $\mathbb{R}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$  in which polynomials can have terms built using function symbols in  $\Omega$  and variables in  $\mathbf{x}, \mathbf{y}, \mathbf{z}$ .

*Problem 2.* Suppose two formulas  $\phi$  and  $\psi$  with  $\phi \wedge \psi \models \perp$ , where  $\phi = f_1 \geq 0 \wedge \dots \wedge f_{r_1} \geq 0 \wedge g_1 > 0 \wedge \dots \wedge g_{s_1} > 0$ ,  $\psi = f_{r_1+1} \geq 0 \wedge \dots \wedge f_r \geq 0 \wedge g_{s_1+1} > 0 \wedge \dots \wedge g_s > 0$ , where  $f_1, \dots, f_r, g_1, \dots, g_s$  are all CQ polynomial,  $f_1, \dots, f_{r_1}, g_1, \dots, g_{s_1} \in \mathbb{R}[\mathbf{x}, \mathbf{y}]^{\Omega_{12}}$ ,  $f_{r_1+1}, \dots, f_r, g_{s_1+1}, \dots, g_s \in \mathbb{R}[\mathbf{x}, \mathbf{z}]^{\Omega_{13}}$ , the goal is to generate an interpolant  $I$  for  $\phi$  and  $\psi$ , expressed using the common symbols  $\mathbf{x}, \Omega_1$ , i.e.,  $I$  includes only polynomials in  $\mathbb{R}[\mathbf{x}]^{\Omega_1}$ .

**Flatten and Purify:** Purify and flatten the formulas  $\phi$  and  $\psi$  by introducing fresh variables for each term with uninterpreted symbols as well as for the terms with uninterpreted symbols. Keep track of new variables introduced exclusively for  $\phi$  and  $\psi$  as well as new common variables.

Let  $\bar{\phi} \wedge \bar{\psi} \wedge \bigwedge D$  be obtained from  $\phi \wedge \psi$  by flattening and purification where  $D$  consists of unit clauses of the form  $\omega(c_1, \dots, c_n) = c$ , where  $c_1, \dots, c_n$  are variables and  $\omega \in \Omega$ . Following [21, 17], using the axiom of an uninterpreted function symbol, a set  $N$  of Horn clauses are generated as follows,

$$N = \left\{ \bigwedge_{k=1}^n c_k = b_k \rightarrow c = b \mid \omega(c_1, \dots, c_n) = c \in D, \omega(b_1, \dots, b_n) = b \in D \right\}.$$

The set  $N$  is partitioned into  $N_{\phi}, N_{\psi}, N_{\text{mix}}$  with all symbols in  $N_{\phi}, N_{\psi}$  appearing in  $\bar{\phi}, \bar{\psi}$ , respectively, and  $N_{\text{mix}}$  consisting of symbols from both  $\bar{\phi}, \bar{\psi}$ .

It is easy to see that for every Horn clause in  $N_{\text{mix}}$ , each of equalities in the hypothesis as well as conclusion is mixed.

$$\phi \wedge \psi \models \perp \text{ iff } \bar{\phi} \wedge \bar{\psi} \wedge D \models \perp \text{ iff } (\bar{\phi} \wedge N_{\phi}) \wedge (\bar{\psi} \wedge N_{\psi}) \wedge N_{\text{mix}} \models \perp. \quad (31)$$

Notice that  $\bar{\phi} \wedge \bar{\psi} \wedge N \models \perp$  has no uninterpreted function symbols. An interpolant generated for this problem<sup>7</sup> can be used to generate an interpolant for  $\phi, \psi$  after uniformly replacing all new symbols by their corresponding expressions from  $D$ .

<sup>7</sup> after properly handling  $N_{\text{mix}}$  since Horn clauses have symbols both from  $\bar{\phi}$  and  $\bar{\psi}$ .

## 5.2 Combination algorithm

If  $N_{\text{mix}}$  is empty, implying there are no mixed Horn clauses, then the algorithm invokes **IGFQC** on a finite set of subproblems generated from a disjunction of conjunction of polynomial inequalities obtained after expanding Horn clauses in  $N_\phi$  and  $N_\psi$  and applying De Morgan's rules. The resulting interpolant is a disjunction of the interpolants generated for each subproblem.

The case when  $N_{\text{mix}}$  is nonempty is more interesting, but it has the same structure as the algorithm  $\text{INTER}_{LI(Q)^S}$  in [17] except that instead of  $\text{INTER}_{LI(Q)}$ , it calls **IGFQC**.

The following lemma proves that if a conjunction of polynomial inequalities satisfies the **NSOSC** condition and an equality on variables can be deduced from it, then it suffices to consider only linear inequalities in the conjunction. This property enables us to use algorithms used in [17] to generate such equalities as well as separating terms for the constants appearing in mixed equalities (algorithm **SEP** in [17]).

**Lemma 9.** *Let  $f_i$ ,  $i = 1, \dots, r$  be CQ polynomials, and  $\lambda_i \geq 0$ , if  $\sum_{i=1}^r \lambda_i f_i \equiv 0$ , then for any  $1 \leq i \leq r$ ,  $\lambda_i = 0$  or  $f_i$  is linear.*

*Proof.* Let  $f_i = \mathbf{x}^T A_i \mathbf{x} + l_i^T \mathbf{x} + \gamma_i$ , then  $A_i \preceq 0$ , for  $i = 1, \dots, r$ . Since  $\sum_{i=1}^r \lambda_i f_i = 0$ , we have  $\sum_{i=1}^r \lambda_i A_i = 0$ . Thus for any  $1 \leq i \leq r$ ,  $\lambda_i = 0$  or  $A_i = 0$ .  $\square$

**Lemma 10.** *Let  $\bar{\phi}$  and  $\bar{\psi}$  be obtained as above with **NSOSC**. If  $\bar{\phi} \wedge \bar{\psi}$  is satisfiable,  $\bar{\phi} \wedge \bar{\psi} \models c_k = b_k$ , then  $LP(\bar{\phi}) \wedge LP(\bar{\psi}) \models c_k = b_k$ , where  $LP(\bar{\phi})$  ( $LP(\bar{\psi})$ ) is a formula defined by all the linear constraints in  $\bar{\phi}$  ( $\bar{\psi}$ ).*

*Proof.* Since  $\bar{\phi} \wedge \bar{\psi} \models c_k = b_k$ , then  $\bar{\phi} \wedge \bar{\psi} \wedge c_k > b_k \models \perp$ . By Theorem 4, there exist  $\lambda_i \geq 0$  ( $i = 1, \dots, r$ ),  $\eta_j \geq 0$  ( $j = 0, 1, \dots, s$ ),  $\eta \geq 0$  and two quadratic SOS polynomials  $\bar{h}_1$  and  $\bar{h}_2$  such that

$$\sum_{i=1}^r \lambda_i \bar{f}_i + \sum_{j=1}^s \eta_j \bar{g}_j + \eta(c_k - b_k) + \eta_0 + \bar{h}_1 + \bar{h}_2 \equiv 0, \quad (32)$$

$$\eta_0 + \eta_1 + \dots + \eta_s + \eta = 1. \quad (33)$$

As  $\bar{\phi} \wedge \bar{\psi}$  is satisfiable and  $\bar{\phi} \wedge \bar{\psi} \models c_k = b_k$ , there exist  $\mathbf{x}_0, \mathbf{y}_0, \mathbf{z}_0, \mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0$  s.t.  $\bar{\phi}[\mathbf{x}/\mathbf{x}_0, \mathbf{y}/\mathbf{y}_0, \mathbf{a}/\mathbf{a}_0, \mathbf{c}/\mathbf{c}_0]$ ,  $\bar{\psi}[\mathbf{x}/\mathbf{x}_0, \mathbf{z}/\mathbf{z}_0, \mathbf{b}/\mathbf{b}_0, \mathbf{c}/\mathbf{c}_0]$ , and  $c_k = b_k[\mathbf{a}/\mathbf{a}_0, \mathbf{b}/\mathbf{b}_0, \mathbf{c}/\mathbf{c}_0]$ . Thus, it follows that  $\eta_0 = \eta_1 = \dots = \eta_s = 0$  from (32) and  $\eta = 1$  from (33). Hence, (32) is equivalent to

$$\sum_{i=1}^r \lambda_i \bar{f}_i + (c_k - b_k) + \bar{h}_1 + \bar{h}_2 \equiv 0. \quad (34)$$

Similarly, we can prove that there exist  $\lambda'_i \geq 0$  ( $i = 1, \dots, r$ ) and two quadratic SOS polynomials  $\bar{h}'_1$  and  $\bar{h}'_2$  such that

$$\sum_{i=1}^r \lambda'_i \bar{f}_i + (b_k - c_k) + \bar{h}'_1 + \bar{h}'_2 \equiv 0. \quad (35)$$

From (34) and (35), it follows

$$\sum_{i=1}^r (\lambda + \lambda'_i) \bar{f}_i + \bar{h}_1 + \bar{h}'_1 + \bar{h}_2 + \bar{h}'_2 \equiv 0. \quad (36)$$

In addition, **NSOSC** implies  $\bar{h}_1 \equiv \bar{h}'_1 \equiv \bar{h}_2 \equiv \bar{h}'_2 \equiv 0$ . So

$$\sum_{i=1}^r \lambda_i \bar{f}_i + (c_k - b_k) \equiv 0, \quad (37)$$

and

$$\sum_{i=1}^r \lambda'_i \bar{f}_i + (b_k - c_k) \equiv 0. \quad (38)$$

Applying Lemma 9 to (37), we have that  $\lambda_i = 0$  or  $f_i$  is linear. So

$$LP(\bar{\phi}) \wedge LP(\bar{\psi}) \models c_k \leq b_k.$$

Likewise, by applying Lemma 9 to (38), we have

$$LP(\bar{\phi}) \wedge LP(\bar{\psi}) \models c_k \geq b_k. \quad \square$$

If **NSOSC** is not satisfied, then the recursive call to **IGFQC** can generate linear equalities as stated in Theorems 6 and 7 which can make hypotheses in a Horn clause in  $N_{\text{mix}}$  true, thus deducing a mixed equality on symbols .

---

**Algorithm 3: IGFQCEunmixed**

---

**input** : two formulas  $\bar{\phi}, \bar{\psi}$ , which are constructed respectively from  $\phi$  and  $\psi$  by flattening and purification,

$N_\phi$  : instances of functionality axioms for functions in  $D_\phi$ ,

$N_\psi$  : instances of functionality axioms for functions in  $D_\psi$ ,

where  $\bar{\phi} \wedge \bar{\psi} \wedge N_\phi \wedge N_\psi \models \perp$ ,

**output**: A formula  $I$  to be a Craig interpolant for  $\phi$  and  $\psi$ .

- 1 Transform  $\bar{\phi} \wedge N_\phi$  to a DNF  $\bigvee_i \phi_i$ ;
  - 2 Transform  $\bar{\psi} \wedge N_\psi$  to a DNF  $\bigvee_j \psi_j$ ;
  - 3 **return**  $I := \bigvee_i \wedge_j \mathbf{IGFQC}(\phi_i, \psi_j)$
- 

**Theorem 12.** (*Soundness and Completeness of IGFQCE*) **IGFQCE** computes an interpolant  $I$  of mutually contradictory  $\phi, \psi$  with *CQ* polynomial inequalities and *EUF*.

*Proof.* Let  $\phi$  and  $\psi$  are two formulas satisfy the conditions of the input of the Algorithm **IGFQCE**,  $D$  is the set of definitions of fresh variables introduced during flattening and

---

**Algorithm 4: IGFQCE**


---

**input** :  $\bar{\phi}$  and  $\bar{\psi}$ : two formulas, which are constructed respective from  $\phi$  and  $\psi$  by flattening and purification,  
 $D$  : definitions for fresh variables introduced during flattening and purifying  $\phi$  and  $\psi$ ,  
 $N$  : instances of functionality axioms for functions in  $D$ ,  
 where  $\phi \wedge \psi \models \perp$ ,  
 $\bar{\phi} = f_1 \geq 0 \wedge \dots \wedge f_{r_1} \geq 0 \wedge g_1 > 0 \wedge \dots \wedge g_{s_1} > 0$ ,  
 $\bar{\psi} = f_{r_1+1} \geq 0 \wedge \dots \wedge f_r \geq 0 \wedge g_{s_1+1} > 0 \wedge \dots \wedge g_s > 0$ , where  
 $f_1, \dots, f_r, g_1, \dots, g_s$  are all CQ polynomial,  
 $f_1, \dots, f_{r_1}, g_1, \dots, g_{s_1} \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$ , and  
 $f_{r_1+1}, \dots, f_r, g_{s_1+1}, \dots, g_s \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$   
**output**: A formula  $I$  to be a Craig interpolant for  $\phi$  and  $\psi$

```

1 if NSOSC holds then
2    $L_1 := LP(\bar{\phi}); L_2 := LP(\bar{\psi});$ 
3   separate  $N$  to  $N_\phi, N_\psi$  and  $N_{mix}$ ;
4    $N_\phi, N_\psi := \text{SEPMix}(L_1, L_2, \emptyset, N_\phi, N_\psi, N_{mix});$ 
5    $\bar{I} := \text{IGFQCEunmixed}(\bar{\phi}, \bar{\psi}, N_\phi, N_\psi);$ 
6 else
7   Find  $\delta_1, \dots, \delta_r \geq 0$  and an SOS polynomial  $h$  using SDP s.t.  $\sum_{i=1}^r \delta_i f_i + h \equiv 0$ ;
8   Construct  $h_1 \in \mathbb{R}[\mathbf{x}, \mathbf{y}]$  and  $h_2 \in \mathbb{R}[\mathbf{x}, \mathbf{z}]$  with form (H1) and (H2);
9    $f := \sum_{i=1}^{r_1} \delta_i f_i + h_1 = -\sum_{i=r_1+1}^r \delta_i f_i - h_2$ ;
10  Construct  $\bar{\phi}'$  and  $\bar{\psi}'$  by Theorem 6 and Theorem 7 by eliminating variables due to
    condition  $h_1 = h_2 = 0$ ;
11   $I' := \text{IGFQCE}(\bar{\phi}', \bar{\psi}', D, N);$ 
12   $\bar{I} := (f > 0) \vee (f \geq 0 \wedge I')$ ;
13 end
14 Obtain  $I$  from  $\bar{I}$ ;
15 return  $I$ 

```

---

purifying  $\phi$  and  $\psi$ , and  $N$  is the set of instances of functionality axioms for functions in  $D$ .

If the condition **NSOSC** is satisfied, then from Lemma 10, we could deal with  $N$  just using the linear constraints in  $\phi$  and  $\psi$ , which is the same as [17]. Since  $N$  is easy to be divided into three parts,  $N_\phi \wedge N_\psi \wedge N_{mix}$ . From the algorithm in [17],  $N_{mix}$  can be divided into two parts  $N_\phi^{mix}$  and  $N_\psi^{mix}$  and add them to  $N_\phi$  and  $N_\psi$ , respectively. Thus, we have

$$\begin{aligned}
\phi \wedge \psi \models \perp &\Leftrightarrow \bar{\phi} \wedge \bar{\psi} \wedge D \models \perp \Leftrightarrow \bar{\phi} \wedge \bar{\psi} \wedge N_\phi \wedge N_\psi \wedge N_{mix} \models \perp \\
&\Leftrightarrow \bar{\phi} \wedge N_\phi \wedge N_\phi^{mix} \wedge \bar{\psi} \wedge N_\psi \wedge N_\psi^{mix} \models \perp.
\end{aligned}$$

The correctness of step 4 is guaranteed by Lemma 10 and Theorem 8 in [17]. After step 4,  $N_\phi$  is replaced by  $N_\phi \wedge N_\phi^{mix}$ , and  $N_\psi$  is replaced by  $N_\psi \wedge N_\psi^{mix}$ . An interpolant for  $\bar{\phi} \wedge N_\phi \wedge N_\phi^{mix}$  and  $\bar{\psi} \wedge N_\psi \wedge N_\psi^{mix}$  is generated in step 5, the correctness of this step is guaranteed by Theorem 9. Otherwise if the condition **NSOSC** is not satisfied, we

---

**Algorithm 5: SEPmix**

---

**input** :  $L_1, L_2$ : two sets of linear inequalities,  
 $W$ : a set of equalities,  
 $N_\phi, N_\psi, N_{mix}$ : three sets of instances of functionality axioms.  
**output**:  $N_\phi, N_\psi$ : s.t.  $N_{mix}$  is separated into  $N_\phi$  or  $N_\psi$ .

```
1 if there exists  $(\bigwedge_{k=1}^K c_k = b_k \rightarrow c = b) \in N_{mix}$  s.t.  $L_1 \wedge L_2 \wedge W \models \bigwedge_{k=1}^K c_k = b_k$  then
2   if  $c$  is  $\phi$ -local and  $b$  is  $\psi$ -local then
3     for each  $k \in \{1, \dots, K\}$ ,  $t_k^-, t_k^+ := \text{SEP}(L_1, L_2, c_k, b_k)$ ;
4      $\alpha :=$  function symbol corresponding to  $\bigwedge_{k=1}^K c_k = b_k \rightarrow c = b$ ;
5      $t :=$  fresh variable;  $D := D \cup \{t = f(t_1^+, \dots, t_K^+)\}$ ;
6      $C_\phi := \bigwedge_{k=1}^K c_k = t_k^+ \rightarrow c = t$ ;  $C_\psi := \bigwedge_{k=1}^K t_k^+ = b_k \rightarrow t = b$ ;
7      $N_{mix} := N_{mix} - \{C\}$ ;  $N_\phi := N_\phi \cup \{C_\phi\}$ ;
8      $N_\psi := N_\psi \cup \{C_\psi\}$ ;  $W := W \cup \{c = t, t = d\}$ ;
9   else
10    if  $c$  and  $b$  are  $\phi$ -local then
11       $N_{mix} := N_{mix} - \{C\}$ ;  $N_\phi := N_\phi \cup \{C\}$ ;  $W := W \cup \{c = b\}$ ;
12    else
13       $N_{mix} := N_{mix} - \{C\}$ ;  $N_\phi := N_\phi \cup \{C\}$ ;  $W := W \cup \{c = b\}$ ;
14    end
15  end
16  call SEPmix( $L_1, L_2, W, N_\phi, N_\psi, N_{mix}$ );
17 else
18   return  $N_\phi$  and  $N_\psi$ ;
19 end
```

---

---

**Algorithm 6: SEP**

---

**input** :  $L_1, L_2$ : two sets of linear inequalities,  
 $c_k, b_k$ : local variables from  $L_1$  and  $L_2$  respectively.  
**output**:  $t^-, t^+$ : expressions over common variables of  $L_1$  and  $L_2$  s.t.  $L_1 \models t^- \leq c_k \leq t^+$   
and  $L_2 \models t^+ \leq b_k \leq t^-$

```
1 rewrite  $L_1$  and  $L_2$  as constraints in matrix form  $a - Ax \geq 0$  and  $b - Bx \geq 0$ ;
2  $x_i, x_j$  in  $x$  is the variable  $c_k$  and  $b_k$ ;
3  $e^+ := \nu^+ A + \mu^+ B$ ;  $e^- := \nu^- A + \mu^- B$ ;
4  $\nu^+, \mu^+ :=$  solution for
    $\nu^+ \geq 0 \wedge \mu^+ \geq 0 \wedge \nu^+ a + \mu^+ b \leq 0 \wedge e_i^+ = 1 \wedge e_j^+ = -1 \wedge \bigwedge_{l \neq i, j} e_l^+ = 0$ ;
5  $\nu^-, \mu^- :=$  solution for
    $\nu^- \geq 0 \wedge \mu^- \geq 0 \wedge \nu^- a + \mu^- b \leq 0 \wedge e_i^- = -1 \wedge e_j^- = 1 \wedge \bigwedge_{l \neq i, j} e_l^- = 0$ ;
6  $t^+ := \mu^+ Bx + x_j - \mu^+ b$ ;
7  $t^- := \nu^- Ax + x_i - \nu^- a$ ;
8 return  $t^+$  and  $t^-$ ;
```

---

can obtain two polynomials  $h_1$  and  $h_2$ , and derive two formulas  $\bar{\phi}'$  and  $\bar{\psi}'$ . By Theorem 5, if there is an interpolant  $I'$  for  $\bar{\phi}'$  and  $\bar{\psi}'$ , then we can get an interpolant  $I$  for  $\bar{\phi}$  and  $\bar{\psi}$  at step 11. Similar to the proof of Theorem 9, it is easy to argue that this reduction

will terminate at the case when **NSOSC** holds in finite steps. Thus, this completes the proof.  $\square$

*Example 3.* Let two formulae  $\phi$  and  $\psi$  be defined as follows,

$$\begin{aligned}\phi := & (f_1 = -(y_1 - x_1 + 1)^2 - x_1 + x_2 \geq 0) \wedge (y_2 = \alpha(y_1) + 1) \\ & \wedge (g_1 = -x_1^2 - x_2^2 - y_2^2 + 1 > 0),\end{aligned}$$

$$\begin{aligned}\psi := & (f_2 = -(z_1 - x_2 + 1)^2 + x_1 - x_2 \geq 0) \wedge (z_2 = \alpha(z_1) - 1) \\ & \wedge (g_2 = -x_1^2 - x_2^2 - z_2^2 + 1 > 0),\end{aligned}$$

where  $\alpha$  is an uninterpreted function. Then

$$\begin{aligned}\bar{\phi} := & (f_1 = -(y_1 - x_1 + 1)^2 - x_1 + x_2 \geq 0) \wedge (y_2 = y + 1) \\ & \wedge (g_1 = -x_1^2 - x_2^2 - y_2^2 + 1 > 0), \\ \bar{\psi} := & (f_2 = -(z_1 - x_2 + 1)^2 + x_1 - x_2 \geq 0) \wedge (z_2 = z - 1) \\ & \wedge (g_2 = -x_1^2 - x_2^2 - z_2^2 + 1 > 0), \\ D = & (y_1 = z_1 \rightarrow y = z).\end{aligned}$$

The condition **NSOSC** is not satisfied, since  $-f_1 - f_2 = (y_1 - x_1 + 1)^2 + (z_1 - x_2 + 1)^2$  is a SOS. It is easy to have

$$h_1 = (y_1 - x_1 + 1)^2, \quad h_2 = (z_1 - x_2 + 1)^2.$$

Let  $f := f_1 + h_1 = -f_2 - h_2 = -x_1 + x_2$ , then it is easy to see that

$$\phi \models f \geq 0, \quad \psi \models f \leq 0.$$

Next we turn to find an interpolant for the following formulae

$$((\phi \wedge f > 0) \vee (\phi \wedge f = 0)) \text{ and } ((\psi \wedge -f > 0) \vee (\psi \wedge f = 0)).$$

Then

$$(f > 0) \vee (f \geq 0 \wedge I_2) \tag{39}$$

is an interpolant for  $\phi$  and  $\psi$ , where  $I_2$  is an interpolant for  $\phi \wedge f = 0$  and  $\psi \wedge f = 0$ . It is easy to see that

$$\phi \wedge f = 0 \models y_1 = x_1 - 1, \quad \psi \wedge f = 0 \models z_1 = x_2 - 1.$$

Substitute then into  $f_1$  in  $\bar{\phi}$  and  $\bar{\psi}$ , we have

$$\begin{aligned}\bar{\phi}' = & -x_1 + x_2 \geq 0 \wedge y_2 = y + 1 \wedge g_1 > 0 \wedge y_1 = x_1 - 1, \\ \bar{\psi}' = & x_1 - x_2 \geq 0 \wedge z_2 = z - 1 \wedge g_2 > 0 \wedge z_1 = x_2 - 1.\end{aligned}$$

Only using the linear form in  $\overline{\phi'}$  and  $\overline{\psi'}$  we deduce that  $y_1 = z_1$  as

$$\overline{\phi'} \models t^- = x_1 - 1 \leq y_1 \leq t^+ = x_2 - 1, \quad \overline{\psi'} \models x_2 - 1 \leq z_1 \leq x_1 - 1.$$

Let  $t = \alpha(t)$ , then separate  $y_1 = z_1 \rightarrow y = z$  into two parts,

$$y_1 = t^+ \rightarrow y = t, \quad t^+ = z_1 \rightarrow t = z.$$

Add them to  $\overline{\phi'}$  and  $\overline{\psi'}$  respectively, we have

$$\begin{aligned} \overline{\phi'}_1 &= -x_1 + x_2 \geq 0 \wedge y_2 = y + 1 \wedge g_1 > 0 \wedge y_1 = x_1 - 1 \wedge y_1 = x_2 - 1 \rightarrow y = t, \\ \overline{\psi'}_1 &= x_1 - x_2 \geq 0 \wedge z_2 = z - 1 \wedge g_2 > 0 \wedge z_1 = x_2 - 1 \wedge x_2 - 1 = z_1 \rightarrow t = z. \end{aligned}$$

Then

$$\begin{aligned} \overline{\phi'}_1 &= -x_1 + x_2 \geq 0 \wedge y_2 = y + 1 \wedge g_1 > 0 \wedge y_1 = x_1 - 1 \wedge \\ &\quad (x_2 - 1 > y_1 \vee y_1 > x_2 - 1 \vee y = t), \\ \overline{\psi'}_1 &= x_1 - x_2 \geq 0 \wedge z_2 = z - 1 \wedge g_2 > 0 \wedge z_1 = x_2 - 1 \wedge t = z. \end{aligned}$$

Thus,

$$\begin{aligned} \overline{\phi'}_1 &= \overline{\phi'}_2 \vee \overline{\phi'}_3 \vee \overline{\phi'}_4, \\ \overline{\phi'}_2 &= -x_1 + x_2 \geq 0 \wedge y_2 = y + 1 \wedge g_1 > 0 \wedge y_1 = x_1 - 1 \wedge x_2 - 1 > y_1, \\ \overline{\phi'}_3 &= -x_1 + x_2 \geq 0 \wedge y_2 = y + 1 \wedge g_1 > 0 \wedge y_1 = x_1 - 1 \wedge y_1 > x_2 - 1, \\ \overline{\phi'}_4 &= -x_1 + x_2 \geq 0 \wedge y_2 = y + 1 \wedge g_1 > 0 \wedge y_1 = x_1 - 1 \wedge y = t. \end{aligned}$$

Since  $\overline{\phi'}_3 = false$ , then  $\overline{\phi'}_1 = \overline{\phi'}_2 \vee \overline{\phi'}_4$ . Then find interpolant

$$I(\overline{\phi'}_2, \overline{\psi'}_1), \quad I(\overline{\phi'}_4, \overline{\psi'}_1).$$

= replace by two  $\geq$ , like,  $y_1 = x_1 - 1$  replace by  $y_1 \geq x_1 - 1$  and  $x_1 - 1 \geq y_1$ .

Then let  $I_2 = I(\overline{\phi'}_2, \overline{\psi'}_1) \vee I(\overline{\phi'}_4, \overline{\psi'}_1)$  an interpolant is found from (39).

## 6 Proven interpolant

Since our result is obtained by numerical calculation, it can't guard the solution satisfy the constraints strictly. Thus, we should verify the solution obtained from a **SDP** solver to get a proven interpolant. In the end of section 4.2, the remark 1 said one can use Lemma 5 to verify the result obtained from some **SDP** solver. In this section, we illuminate how to verify the result obtained from some **SDP** solver to get a proven interpolant by an example.

*Example 4.*

$$\begin{aligned} \phi &: f_1 = 4 - (x - 1)^2 - 4y^2 \geq 0 \wedge f_2 = y - \frac{1}{2} \geq 0, \\ \psi &: f_3 = 4 - (x + 1)^2 - 4y^2 \geq 0 \wedge f_4 = x + 2y \geq 0. \end{aligned}$$

Constructing SOS constraints as following,

$$\begin{aligned} \lambda_1 \geq 0, \lambda_2 \geq 0, \lambda_3 \geq 0, \lambda_4 \geq 0, \\ -(\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 + \lambda_4 f_4 + 1) \text{ is a SOS polynomial} \end{aligned}$$

Using the **SDP** solver *Yalmip* to solve the above constraints for  $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ , take two decimal places, we obtain

$$\lambda_1 = 3.63, \lambda_2 = 38.39, \lambda_3 = 0.33, \lambda_4 = 12.70.$$

Then we have,

$$-(\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 + \lambda_4 f_4 + 1) = 3.96x^2 + 6.10x + 15.84y^2 - 12.99y + 6.315.$$

Using Lemma 5, we have

$$3.96x^2 + 6.10x + 15.84y^2 - 12.99y + 6.315 = 3.96(x + \frac{305}{396})^2 + 15.84(y + \frac{1299}{3168})^2 + \frac{825383}{6336},$$

which is a SOS polynomial obviously. Thus,  $I := \lambda_1 f_1 + \lambda_2 f_2 + 1 > 0$ , i.e.,  $-3.63X^2 - 14.52y^2 + 7.26x + 38.39y - 7.305 > 0$ , is a proven interpolant for  $\phi$  and  $\psi$ .

## 7 Beyond concave quadratic polynomials

Theoretically speaking, *concave quadratic* is quite restrictive. But in practice, the results obtained above are powerful enough to scale up the existing verification techniques of programs and hybrid systems, as all well-known abstract domains, e.g. *octagon*, *polyhedra*, *ellipsoid*, etc. are concave quadratic, which will be further demonstrated in the case study below. Nonetheless, we now discuss how to generalize our approach to more general formulas by allowing polynomial equalities whose polynomials may be neither concave nor quadratic using Gröbner basis.

Let's start the discussion with the following running example.

*Example 5.* Let  $G = A \wedge B$ , where

$$\begin{aligned} A : x^2 + 2x + (\alpha(\beta(a)) + 1)^2 \leq 0 \wedge \beta(a) = 2c + z \wedge \\ 2c^2 + 2c + y^2 + z = 0 \wedge -c^2 + y + 2z = 0, \\ B : x^2 - 2x + (\alpha(\gamma(b)) - 1)^2 \leq 0 \wedge \gamma(b) = d - z \wedge \\ d^2 + d + y^2 + y + z = 0 \wedge -d^2 + y + 2z = 0, \end{aligned}$$

try to find an interpolant for  $A$  and  $B$ .

It is easy to see that there exist some constraints which are not concave quadratic, as some equations are not linear. Thus, the interpolant generation algorithm above is not applicable directly.

For easing discussion, in what follows, we use  $\mathbf{IEq}(S)$ ,  $\mathbf{Eq}(S)$  and  $\mathbf{LEq}(S)$  to stand for the sets of polynomials respectively from inequations, equations and linear equations of  $S$ , for any polynomial formula  $S$ . E.g., in Example 5, we have

$$\begin{aligned} \mathbf{IEq}(A) &= \{x^2 + 2x + (\alpha(\beta(a)) + 1)^2\}, \\ \mathbf{Eq}(A) &= \{\beta(a) - 2c - z, 2c^2 + 2c + y^2 + z, -c^2 + y + 2z\}, \\ \mathbf{LEq}(A) &= \{\beta(a) - 2c - z\}. \end{aligned}$$



In the following, we will use Example 5 as a running example to explain the basic idea how to apply Gröbner basis method to extend our approach to more general polynomial formulas.

Step 1: Flatten and purify. Similar to the concave quadratic case, we purify and flatten  $A$  and  $B$  by introducing fresh variables  $a_1, a_2, b_1, b_2$ , and obtain

$$\begin{aligned} A_0 : & x^2 + 2x + (a_2 + 1)^2 \leq 0 \wedge a_1 = 2c + z \wedge \\ & 2c^2 + 2c + y^2 + z = 0 \wedge -c^2 + y + 2z = 0, \\ D_A : & a_1 = \beta(a) \wedge a_2 = \alpha(a_1), \\ B_0 : & x^2 - 2x + (b_2 - 1)^2 \leq 0 \wedge b_1 = d - z \wedge \\ & d^2 + d + y^2 + y + 2z = 0 \wedge -d^2 + y + z = 0, \\ D_B : & b_1 = \gamma(b) \wedge b_2 = \alpha(b_1). \end{aligned}$$

Step 2: Hierarchical reasoning. Obviously,  $A \wedge B$  is unsatisfiable in  $\mathbf{PT}(\mathbb{Q})^{\{\alpha, \beta, \gamma\}}$  if and only if  $A_0 \wedge B_0 \wedge N_0$  is unsatisfiable in  $\mathbf{PT}(\mathbb{Q})$ , where  $N_0$  corresponds to the conjunction of Horn clauses constructed from  $D_A \wedge D_B$  using the axioms of uninterpreted functions (see the following table).

| D  | $G_0$  | $N_0$                                   |
|--|--|---|
| $D_A : a_1 = \beta(a) \wedge a_2 = \alpha(a_1)$  | $A_0 : x^2 + 2x + (a_2 + 1)^2 \leq 0 \wedge a_1 = 2c + z \wedge 2c^2 + 2c + y^2 + z = 0 \wedge -c^2 + y + 2z = 0$  | $N_0 : b_1 = a_1 \rightarrow b_2 = a_2$ |
| $D_B : b_1 = \gamma(b) \wedge b_2 = \alpha(b_1)$ | $B_0 : x^2 - 2x + (b_2 - 1)^2 \leq 0 \wedge b_1 = d - z \wedge d^2 + d + y^2 + y + 2z = 0 \wedge -d^2 + y + z = 0$ |   |

To prove  $A_0 \wedge B_0 \wedge N_0 \models \perp$ , we compute the Grobner basis of  $\mathbb{G}$  of  $\mathbf{Eq}(A_0) \cup \mathbf{Eq}(B_0)$  under the order  $c \succ d \succ y \succ z \succ a_1 \succeq b_1$ , and have  $a_1 - b_1 \in \mathbb{G}$ . That is,  $A_0 \wedge B_0 \models a_1 = b_1$ . Thus,  $A_0 \wedge B_0 \wedge N_0$  entails

$$a_2 = b_2 \wedge x^2 + 2x + (a_2 + 1)^2 \leq 0 \wedge x^2 - 2x + (b_2 - 1)^2 \leq 0.$$

This implies

$$2x^2 + a_2^2 + b_2^2 + 2 \leq 0,$$

which is obviously unsatisfiable in  $\mathbb{Q}$ .

Step 2 gives a proof of  $A \wedge B \models \perp$ . In order to find an interpolant for  $A$  and  $B$ , we need to divide  $N_0$  into two parts,  $A$ -part and  $B$ -part, i.e., to find a term  $t$  only with common symbols, such that

$$A_0 \models a_1 = t \quad B_0 \models b_1 = t.$$

Then we can choose a new variable  $\alpha_t = \alpha(t)$  to be a common variable, since the term  $t$  and the function  $\alpha$  both are common. Thus  $N_0$  can be divided into two parts as follows,

$$a_2 = \alpha_t \wedge b_2 = \alpha_t.$$

Finally, if we can find an interpolant  $I(x, y, z, \alpha_t)$  for

$$(\mathbf{IEq}(A_0) \wedge \mathbf{LEq}(A_0) \wedge a_2 = \alpha_t) \wedge (\mathbf{IEq}(A_0) \wedge \mathbf{LEq}(A_0) \wedge b_2 = \alpha_t),$$

using Algorithm **IGFQC**, then  $I(x, y, z, \alpha(t))$  will be an interpolant for  $A \wedge B$ .

Step 3: Dividing  $N_0$  into two parts. According to the above analysis, we need to find a witness  $t$  such that  $A_0 \models a_1 = t$ ,  $B_0 \models b_1 = t$ , where  $t$  is an expression over the common symbols of  $A$  and  $B$ . Fortunately, such  $t$  can be computed by Gröbner basis method as follows: First, with the variable order  $c \succ a_1 \succ y \succ z$ , the Gröbner basis  $\mathbb{G}_1$  of  $\mathbf{Eq}(A_0)$  is computed to be

$$\begin{aligned} \mathbb{G}_1 = \{ & y^4 + 4y^3 + 10y^2z + 4y^2 + 20yz + 25z^2 - 4y - 8z, \\ & y^2 + a_1 + 2y + 4z, y^2 + 2c + 2y + 5z \}. \end{aligned}$$

Thus, we have

$$A_0 \models a_1 = -y^2 - 2y - 4z. \quad (40)$$

Similarly, with the variable order  $d \succ b_1 \succ y \succ z$ , the Gröbner basis  $\mathbb{G}_2$  of  $\mathbf{Eq}(B_0)$  is computed to be

$$\begin{aligned} \mathbb{G}_2 = \{ & y^4 + 4y^3 + 6y^2z + 4y^2 + 12yz + 9z^2 - y - z, \\ & y^2 + b_1 + 2y + 4z, y^2 + d + 2y + 3z \}. \end{aligned}$$

Thus, we have

$$B_0 \models b_1 = -y^2 - 2y - 4z. \quad (41)$$

Whence,  $t = -y^2 - 2y - 4z$  is the witness. Let  $\alpha_t = \alpha(-y^2 - 2y - 4z)$ , which is an expression constructed from the common symbols of  $A$  and  $B$ .

Next, find an interpolant for following formula

$$(\mathbf{IEq}(A_0) \wedge \mathbf{LEq}(A_0) \wedge a_2 = \alpha_t) \wedge (\mathbf{IEq}(B_0) \wedge \mathbf{LEq}(B_0) \wedge b_2 = \alpha_t).$$

Using **IGFQC**, we obtain an interpolant for the above formula as

$$I(x, y, z, \alpha_t) = x^2 + 2x + (\alpha_t + 1) \leq 0.$$

Thus,  $x^2 + 2x + (\alpha(-y^2 - 2y - 4z) + 1) \leq 0$  is an interpolant for  $A \wedge B$ .

**Problem 3.** Generally, let  $A(\mathbf{x}, \mathbf{z})$  and  $B(\mathbf{y}, \mathbf{z})$  be

$$\begin{aligned} A : & f_1(\mathbf{x}, \mathbf{z}) \geq 0 \wedge \dots \wedge f_{r_1}(\mathbf{x}, \mathbf{z}) \geq 0 \wedge g_1(\mathbf{x}, \mathbf{z}) > 0 \wedge \dots \wedge g_{s_1}(\mathbf{x}, \mathbf{z}) > 0 \\ & \wedge h_1(\mathbf{x}, \mathbf{z}) = 0 \wedge \dots \wedge h_{p_1}(\mathbf{x}, \mathbf{z}) = 0, \end{aligned} \quad (42)$$

$$\begin{aligned} B : & f_{r_1+1}(\mathbf{y}, \mathbf{z}) \geq 0 \wedge \dots \wedge f_r(\mathbf{y}, \mathbf{z}) \geq 0 \wedge g_{s_1+1}(\mathbf{y}, \mathbf{z}) > 0 \wedge \dots \wedge g_s(\mathbf{y}, \mathbf{z}) > 0 \\ & \wedge h_{p_1+1}(\mathbf{y}, \mathbf{z}) = 0 \wedge \dots \wedge h_p(\mathbf{y}, \mathbf{z}) = 0, \end{aligned} \quad (43)$$

where  $f_1, \dots, f_r$  and  $g_1, \dots, g_s$  are concave quadratic polynomials,  $h_1, \dots, h_t$  are general polynomials, unnecessary to be concave quadratic, and

$$A(\mathbf{x}, \mathbf{z}) \wedge B(\mathbf{y}, \mathbf{z}) \models \perp, \quad (44)$$

try to find an interpolant for  $A(\mathbf{x}, \mathbf{z})$  and  $B(\mathbf{y}, \mathbf{z})$ .

According to the above discussion, Problem 3 can be solved by Algorithm 7 below.

---

**Algorithm 7: IGFQC**

---

**input** : Two formulae  $A, B$  as Problem 3 with  $A \wedge B \models \perp$   
**output**: An formula  $I$  to be a Craig interpolant for  $A$  and  $B$

```
1 Flattening, purification and hierarchical reasoning obtain  $A_0, B_0, N_A, N_B, N_{mix}$ ;  
2  $A_0 := A_0 \wedge N_A, B_0 := B_0 \wedge N_B$ ;  
3 while  $(\mathbf{IEq}(A_0) \wedge \mathbf{LEq}(A_0)) \wedge (\mathbf{IEq}(B_0) \wedge \mathbf{LEq}(B_0)) \not\models \perp$  do  
4   if  $N_{mix} = \emptyset$  then  
5     break  
6   end  
7   Choose a formula  $a_1 = b_1 \rightarrow a_2 = b_2 \in N_{mix}$  corresponding to function  $\alpha$ ;  
8    $N_{mix} := N_{mix} \setminus \{a_1 = b_1 \rightarrow a_2 = b_2\}$ ;  
9   Computing Grobner basis  $\mathbb{G}_1$  for  $\mathbf{Eq}(A_0)$  under purely dictionary ordering with  
   some variable ordering that other local variable  $\succ a_1 \succ$  common variable;  
10  Computing Grobner basis  $\mathbb{G}_2$  for  $\mathbf{Eq}(B_0)$  under purely dictionary ordering with  
   some variable ordering that other local variable  $\succ b_1 \succ$  common variable;  
11  if there exists a expression  $t$  with common variable s.t.  $a_1 \in \mathbb{G}_1 \wedge b_1 \in \mathbb{G}_2$  then  
12    introduce a new variable  $\alpha_t = \alpha(t)$  as a common variable;  
     $A_0 := A_0 \wedge a_2 = \alpha_t, B_0 := B_0 \wedge b_2 = \alpha_t$   
13  end  
14 end  
15 if  $(\mathbf{IEq}(A_0) \wedge \mathbf{LEq}(A_0)) \wedge (\mathbf{IEq}(B_0) \wedge \mathbf{LEq}(B_0)) \models \perp$  then  
16   Using IGFQC to obtain an interpolant  $I_0$  for above formula;  
17   Obtain an interpolant  $I$  for  $A \wedge B$  from  $I_0$ ;  
18   return  $I$   
19 end  
20 else  
21   return Fail  
22 end
```

---

## 8 Implementation and experimental results

We have implemented the presented algorithms in *Mathematica* to synthesize interpolation for concave quadratic polynomial inequalities as well as their combination with *EUF*. To deal with SOS solving and semi-definite programming, the Matlab-based optimization tool *Yalmip* [14] and the SDP solver *SDPT3* [23] are invoked. In what follows we demonstrate our approach by some examples, which have been evaluated on a 64-bit Linux computer with a 2.93GHz Intel Core-i7 processor and 4GB of RAM.

*Example 6.* Consider the example:

$$\phi := (f_1 \geq 0) \wedge (f_2 \geq 0) \wedge (g_1 > 0), \quad \psi := (f_3 \geq 0). \quad \phi \wedge \psi \models \perp.$$

where  $f_1 = x_1, f_2 = x_2, f_3 = -x_1^2 - x_2^2 - 2x_2 - z^2, g_1 = -x_1^2 + 2x_1 - x_2^2 + 2x_2 - y^2$ .

The interpolant returned after 0.394 s is

$$I := \frac{1}{2}x_1^2 + \frac{1}{2}x_2^2 + 2x_2 > 0$$

*Example 7.* Consider the unsatisfiable conjunction  $\phi \wedge \psi$ :

$$\phi := f_1 \geq 0 \wedge f_2 \geq 0 \wedge f_3 \geq 0 \wedge g_1 > 0, \quad \psi := f_4 \geq 0 \wedge f_5 \geq 0 \wedge f_6 \geq 0 \wedge g_2 > 0.$$

where  $f_1 = -y_1 + x_1 - 2$ ,  $f_2 = -y_1^2 - x_1^2 + 2x_1y_1 - 2y_1 + 2x_1$ ,  $f_3 = -y_2^2 - y_1^2 - x_2^2 - 4y_1 + 2x_2 - 4$ ,  $f_4 = -z_1 + 2x_2 + 1$ ,  $f_5 = -z_1^2 - 4x_2^2 + 4x_2z_1 + 3z_1 - 6x_2 - 2$ ,  $f_6 = -z_2^2 - x_1^2 - x_2^2 + 2x_1 + z_1 - 2x_2 - 1$ ,  $g_1 = 2x_2 - x_1 - 1$ ,  $g_2 = 2x_1 - x_2 - 1$ .

The condition NSOSC does not hold, since

$$-(2f_1 + f_2) = (y_1 - x_1 + 2)^2 \text{ is a sum of square.}$$

Then we have  $h = (y_1 - x_1 + 2)^2$ , and

$$h_1 = h = (y_1 - x_1 + 2)^2, \quad h_2 = 0.$$

Let  $f = 2f_1 + f_2 + h_1 = 0$ . Then construct  $\phi'$  by setting  $y_1 = x_1 - 2$  in  $\phi$ ,  $\psi'$  is  $\psi$ . That is

$$\phi' := 0 \geq 0 \wedge 0 \geq 0 \wedge -y_2^2 - x_1^2 - x_2^2 + 2x_2 \geq 0 \wedge g_1 > 0, \quad \psi' := \psi.$$

Then the interpolation for  $\phi$  and  $\psi$  is reduced as

$$I(\phi, \psi) = (f > 0) \vee (f = 0 \wedge I(\phi', \psi')) = I(\phi', \psi').$$

For  $\phi'$  and  $\psi'$ , the condition NSOSC is still unsatisfied, since  $-f_4 - f_5 = (z_1 - 2x_2 - 1)^2$  is an SOS. Then we have  $h = h_2 = (z_1 - 2x_2 - 1)^2$ ,  $h_1 = 0$ , and thus  $f = 0$ .

$$\phi'' = \phi', \quad \psi'' = 0 \geq 0 \wedge 0 \geq 0 \wedge -z_2^2 - x_1^2 - x_2^2 + 2x_1 \geq 0 \wedge g_2 > 0.$$

The interpolation for  $\phi'$  and  $\psi'$  is further reduced by  $I(\phi', \psi') = I(\phi'', \psi'')$ , where

$$\begin{aligned} \phi'' &:= (f'_1 = -y_2^2 - x_1^2 - x_2^2 + 2x_2 \geq 0) \wedge 2x_2 - x_1 - 1 > 0, \\ \psi'' &:= (f'_2 = -z_2^2 - x_1^2 - x_2^2 + 2x_1 \geq 0) \wedge 2x_1 - x_2 - 1 > 0. \end{aligned}$$

Here the condition NSOSC holds for  $\phi''$  and  $\psi''$ , then by SDP we find  $\lambda_1 = \lambda_2 = 0.25$ ,  $\eta_0 = 0$ ,  $\eta_1 = \eta_2 = 0.5$  and SOS polynomials  $h_1 = 0.25 * ((x_1 - 1)^2 + (x_2 - 1)^2 + y_2^2)$  and  $h_2 = 0.25 * ((x_1 - 1)^2 + (x_2 - 1)^2 + z_2^2)$  such that  $\lambda_1 f'_1 + \lambda_2 f'_2 + \eta_0 + \eta_1 g_1 + \eta_2 g_2 + h_1 + h_2 \equiv 0$  and  $\eta_0 + \eta_1 + \eta_2 = 1$ . For  $\eta_0 + \eta_1 = 0.5 > 0$ , the interpolant returned after 2.089 s is  $f > 0$ , i.e.  $I := -x_1 + x_2 > 0$ .

*Example 8.* Consider the example:

$$\begin{aligned} \phi &:= (f_1 = -(y_1 - x_1 + 1)^2 - x_1 + x_2 \geq 0) \wedge (y_2 = \alpha(y_1) + 1) \\ &\quad \wedge (g_1 = -x_1^2 - x_2^2 - y_2^2 + 1 > 0), \\ \psi &:= (f_2 = -(z_1 - x_2 + 1)^2 + x_1 - x_2 \geq 0) \wedge (z_2 = \alpha(z_1) - 1) \\ &\quad \wedge (g_2 = -x_1^2 - x_2^2 - z_2^2 + 1 > 0). \end{aligned}$$

where  $\alpha$  is an uninterpreted function. It takes 0.369 s in our approach to reduce the problem to find an interpolant as  $I(\phi'_2, \bar{\psi}'_1) \vee (\phi'_4, \bar{\psi}'_1)$ , and another 2.029 s to give the final interpolant as

$$I := (-x_1 + x_2 > 0) \vee \left(\frac{1}{4}(-4\alpha(x_2 - 1) - x_1^2 - x_2^2) > 0\right)$$

*Example 9.* Let two formulae  $\phi$  and  $\psi$  be defined as

$$\begin{aligned}\phi &:= (f_1 = 4 - x^2 - y^2 \geq 0) \wedge f_2 = y \geq 0 \wedge (g = x + y - 1 > 0), \\ \psi &:= (f_4 = x \geq 0) \wedge (f_5 = 1 - x^2 - (y + 1)^2 \geq 0).\end{aligned}$$

The interpolant returned after 0.532 s is  $I := \frac{1}{2}(x^2 + y^2 + 4y) > 0$ <sup>8</sup>.

*Example 10.* This is a linear interpolation problem adapted from [17]. Consider the unsatisfiable conjunction  $\phi \wedge \psi$ :

$$\phi := z - x \geq 0 \wedge x - y \geq 0 \wedge -z > 0, \quad \psi := x + y \geq 0 \wedge -y \geq 0.$$

It takes 0.250 s for our approach to give an interpolant as  $I := -0.8x - 0.2y > 0$ .

*Example 11.* Consider another linear interpolation problem combined with *EUF*:

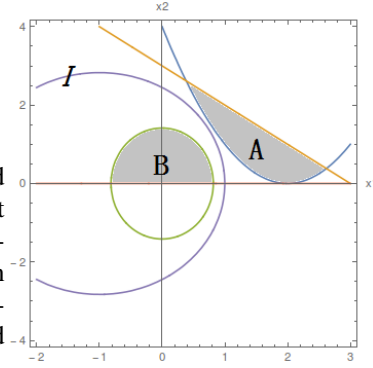
$$\phi := f(x) \geq 0 \wedge x - y \geq 0 \wedge y - x \geq 0, \quad \psi := -f(y) > 0.$$

The interpolant returned after 0.236 s is  $I := f(y) \geq 0$ .

*Example 12.* Consider two formulas  $A$  and  $B$  with  $A \wedge B \models \perp$ , where

$$\begin{aligned}A &:= -x_1^2 + 4x_1 + x_2 - 4 \geq 0 \wedge \\ &\quad -x_1 - x_2 + 3 - y^2 > 0, \\ B &:= -3x_1^2 - x_2^2 + 1 \geq 0 \wedge x_2 - z^2 \geq 0.\end{aligned}$$

Note that a concave quadratic polynomial (the bold one) from the *ellipsoid* domain is involved in  $B$ . It takes 0.388 s using our approach to give an interpolant as  $I := -3 + 2x_1 + x_1^2 + \frac{1}{2}x_2^2 > 0$ . An intuitive description of the interpolant is as the purple curve in the right figure, which separates  $A$  and  $B$  in the panel of common variables  $x_1$  and  $x_2$ .



*Example 13.* Consider two formulas  $\phi$  and  $\psi$  both are defined by an ellipse joint a half-plane:

$$\phi := 4 - (x - 1)^2 - 4y^2 \geq 0 \wedge y - \frac{1}{2} \geq 0, \quad \psi := 4 - (x + 1)^2 - 4y^2 \geq 0 \wedge x + 2y \geq 0.$$

The interpolant returned after 0.248 s is  $I := -3.63x^2 - 14.52y^2 + 7.26x + 38.39y - 7.305 > 0$ .

*Example 14.* Consider two formulas  $\phi$  and  $\psi$  both are defined by an octagon joint a half-plane:

$$\begin{aligned}\phi &:= -3 \leq x \leq 1 \wedge -2 \leq y \leq 2 \wedge -4 \leq x - y \leq 2 \wedge -4 \leq x + y \leq 2 \wedge x + 2y + 1 \leq 0, \\ \psi &:= -1 \leq x \leq 3 \wedge -2 \leq y \leq 2 \wedge -2 \leq x - y \leq 4 \wedge -2 \leq x + y \leq 4 \wedge 2x - 5y + 6 \leq 0.\end{aligned}$$

The interpolant returned after 0.225 s is  $I := -13.42x - 29.23y - 1.7 > 0$ .

<sup>8</sup> In order to give a more objective comparison of performance with the approach proposed in [5], we skip over line 1 in the previous algorithm **IGFQC**.

*Example 15.* Consider two formulas  $\phi$  and  $\psi$  both are defined by an octagon joint a half-plane:

$$\begin{aligned}\phi &:= 2 \leq x \leq 7 \wedge 0 \leq y \leq 3 \wedge 0 \leq x - y \leq 6 \wedge 3 \leq x + y \leq 9 \wedge 23 - 3x - 8y \leq 0, \\ \psi &:= 0 \leq x \leq 5 \wedge 2 \leq y \leq 5 \wedge -4 \leq x - y \leq 2 \wedge 3 \leq x + y \leq 9 \wedge y - 3x - 2 \leq 0.\end{aligned}$$

The interpolant returned after 0.225 s is  $I := 12.3x - 7.77y + 4.12 > 0$ .

| Example    | Type             | Time (sec) |       |        |       |              |
|------------|------------------|------------|-------|--------|-------|--------------|
|            |                  | CLP-PROVER | FOCI  | CSISAT | AiSat | Our Approach |
| Example 6  | NLA              | –          | –     | –      | –     | 0.394        |
| Example 7  | NLA              | –          | –     | –      | –     | 2.089        |
| Example 8  | NLA+ <i>EU</i> F | –          | –     | –      | –     | 2.398        |
| Example 9  | NLA              | –          | –     | –      | 0.023 | 0.532        |
| Example 10 | LA               | 0.023      | ×     | 0.003  | –     | 0.250        |
| Example 11 | LA+ <i>EU</i> F  | 0.025      | 0.006 | 0.007  | –     | 0.236        |
| Example 12 | Ellipsoid        | –          | –     | –      | –     | 0.388        |
| Example 13 | Ellipsoid2       | –          | –     | –      | 0.013 | 0.248        |
| Example 14 | Octagon1         | 0.059      | ×     | 0.004  | 0.021 | 0.225        |
| Example 15 | Octagon2         | 0.065      | ×     | 0.004  | 0.122 | 0.216        |

– means that the interpolant generation fails, and × specifies a particularly wrong answer.

**Table 1.** Evaluation results of the presented examples

The experimental evaluation on the above examples is illustrated in Table 1, where we have also compared on the same platform with the performances of AiSat, a tool for nonlinear interpolant generation proposed in [5], as well as three publicly available interpolation procedures for linear-arithmetic cases, i.e. Rybalchenko’s tool CLP-PROVER in [17], McMillan’s procedure FOCI in [15], and Beyer’s tool CSISAT in [2]. Table 1 shows that our approach can successfully solve all the examples and it is especially the completeness that makes it an extraordinary competitive candidate for synthesizing interpolation. Besides, CLP-PROVER, FOCI, and CSISAT can handle only linear-arithmetic expressions with an efficient optimization (and thus the performances in linear cases are better than our raw implementation). As for AiSat, a rather limited set of applications is acceptable because of the weakness of tackling local variables, and whether an interpolant can be found or not depends on a pre-specified total degree. In [5], not only all the constraints in formula  $\phi$  should be considered but also some of their products, for instance,  $f_1, f_2, f_3 \geq 0$  are three constraints in  $\phi$ , then four constraints  $f_1f_2, f_1f_3, f_2f_3, f_1f_2f_3 \geq 0$  are added in  $\phi$ .

Table 1 indicates the efficiency of our tool is lower than any of other tools whenever a considered example is solvable by both. This is mainly because our tool is implemented in *Mathematica*, and therefore have to invoke some SDP solvers with low efficiency. As a future work, we plan to re-implement the tool using C, thus we can call SDP solver CSDP which is much more efficient. Once a considered problem is linear, an existing interpolation procedure will be invoked directly, thus, SDP solver is not needed.

## 9 Conclusion

The paper proposes a polynomial time algorithm for generating interpolants from mutually contradictory conjunctions of concave quadratic polynomial inequalities over the reals. Under a technical condition that if no nonpositive constant combination of nonstrict inequalities is a sum of squares polynomials, then such an interpolant can be generated essentially using the linearization of quadratic polynomials. Otherwise, if this condition is not satisfied, then the algorithm is recursively called on smaller problems after deducing linear equalities relating variables. The resulting interpolant is a disjunction of conjunction of polynomial inequalities.

Using the hierarchical calculus framework proposed in [21], we give an interpolation algorithm for the combined quantifier-free theory of concave quadratic polynomial inequalities and equality over uninterpreted function symbols. The combination algorithm is patterned after a combination algorithm for the combined theory of linear inequalities and equality over uninterpreted function symbols.

In addition, we also discuss how to extend our approach to formulas with polynomial equalities whose polynomials may be neither concave nor quadratic using Gröbner basis.

The proposed approach is applicable to all existing abstract domains like *octagon*, *polyhedra*, *ellipsoid* and so on, therefore it can be used to improve the scalability of existing verification techniques for programs and hybrid systems.

An interesting issue raised by the proposed framework for dealing with nonlinear polynomial inequalities is the extent to which their linearization with some additional conditions on the coefficients (such as concavity for quadratic polynomials) can be exploited. We are also investigating how results reported for nonlinear polynomial inequalities based on positive nullstellensatz [22] in [5] and the Archimedian condition on variables, implying that every variable ranged over a bounded interval, can be exploited in the proposed framework for dealing with polynomial inequalities.

## References

1. A. Barvinok: A course in convexity. Vol. 54. American Mathematical Soc., 2002.
2. D. Beyer, D. Zufferey, and R. Majumdar: CSIsat: Interpolation for LA+EUF. Proc. *Computer Aided Verification (CAV)*, 2008, Princeton, July 07-14, 2008.
3. CSDP: <http://infohost.nmt.edu/~borchers/csdp.html>.
4. L. Dai, T. Gan, B. Xia and N. Zhan: Barrier certificate revisited. To appear J. of Symbolic Computation. <http://lcs.ios.ac.cn/~znj/papers/jsc14.pdf>.
5. L. Dai, B. Xia, and N. Zhan: Generating non-linear interpolants by semidefinite programming. *Computer Aided Verification*. Springer Berlin Heidelberg, 2013: 364-380.
6. V. D'Silva, M. Purandare, G. Weissenbacher and D. Kroening: Interpolant Strength. *Verification, Model Checking and Abstract Interpretation (VMCAI)*, Springer LNCS 5944, 2010, 129-145.
7. T. Fujie and M. Kojima: Semidefinite programming relaxation for nonconvex quadratic programs. *Journal of Global Optimization*, 367-380, 1997.
8. T. Gan, L. Dai, B. Xia, N. Zhan, D. Kapur and M. Chen: Interpolation synthesis for quadratic polynomial inequalities and combination with EUF. In arXiv:1601.04802, <http://arxiv.org/abs/1601.04802>.
9. D. Kapur: Interpolation and Quantifier Elimination, Draft Working Paper, Department of Computer Science, University of New Mexico, June 2013.

10. D. Kapur, R. Majumdar and C. Zarba: Interpolation for Data Structures, Proceedings of the 14th ACM SIGSOFT Symp. on Foundations of Software Engineering, 2006, Seattle, Washington.
11. J. Krajíček: Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 1997, 62(02): 457-486.
12. S. Kupferschmid and B. Becker: Craig interpolation in the presence of non-linear constraints. *Formal Modeling and Analysis of Timed Systems*. Springer Berlin Heidelberg, 2011: 240-255.
13. M. Laurent: Sums of squares, moment matrices and optimization over polynomials(Updated version) . *Emerging Applications of Algebraic Geometry, Vol. 149 of IMA Volumes in Mathematics and its Applications* 157–270, 2010.
14. J. Löfberg: Pre- and post-processing sum-of-squares programs in practice. *J. of IEEE Transactions on Automatic Control*, 54(5):1007-1011, 2009. <http://users.isy.liu.se/johanl/yalmip/>.
15. K.L. McMillan: An interpolating theorem prover. *Theoretical Computer Science*, 2005, 345(1): 101-121.
16. P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 1997, 62(03): 981-998.
17. A. Rybalchenko and V. Sofronie-Stokkermans.: Constraint solving for interpolation. *Journal of Symbolic Computation* 45,1212-1233 , 2010.
18. A. Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.
19. SeDuMi: <http://sedumi.ie.lehigh.edu>.
20. V. Sofronie-Stokkermans: Hierarchical reasoning in local theory extensions. *Proc. of 20th Intl. Conf. on Automated Deduction (CADE-20)*, LNAI 3632, 219-234.
21. V. Sofronie-Stokkermans: Interpolation in local theory extensions. *J. of Logical Methods in Computer Science*, Vol. 4, No. 1, 2008, 1-31.
22. G. Stengle: A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Math. Ann.*, 1974, 207: 87–97.
23. R. H. Tütüncü, K. C. Toh, and M. J. Todd: Solving semidefinite-quadratic-linear programs using SDPT3. *J. of Mathematical programming*, 95(2):189-217, 2003. <http://www.math.nus.edu.sg/~mattohkc/sdpt3.html>.
24. L. Vandenberghe, S. Boyd: Semidefinite programming[J]. *SIAM review*, 1996, 38(1): 49-95.
25. H. Wolkowicz, R. Saigal, and L. Vandenberghe (eds): *Handbook of semidefinite programming: theory, algorithms, and applications*. Vol. 27. Springer, 2000.
26. G. Yorsh, M. Musuvathi: A combination method for generating interpolants. *Proc. Automated Deduction (CADE)*, 2005, Springer LNCS, 2005: 353-368.
27. H. Zhao, N. Zhan, D. Kapur, and K.G. Larsen: A “Hybrid” Approach for Synthesizing Optimal Controllers of Hybrid Systems: A Case Study of Oil Pump Industrial Example, *Proc. Formal Methods (FM)*, 2012, LNCS, August 2012.
28. H. Zhao, N. Zhan, and D. Kapur: Synthesizing switching controllers for hybrid systems by generating invariants, *Proc. Festschrift Symp. in honor of He Jifeng*, Sept. 01-03, 2013.